LUISS

Corso di laurea in Governo, Amministrazione e Politica

Cattedra di Diritto dell'informazione e della comunicazione

Cavi sottomarini. Dati e infrastrutture per le Comunicazioni e la Difesa

Prof. Maurizio Mensi

RELATORE

Prof. Raffaele Marchetti

CORRELATORE

Guido Ripanti, Matr. 649772

CANDIDATO

Anno Accademico 2022/2023

Sommario

INTRODUZIONE *5*
Obiettivi e rilevanza della ricerca 7
CAPITOLO 1 CAVI E DATI *11*
1.1 NOZIONI E TIPOLOGIE **11**
1.1.1 Cavi energetici e cavi in fibra ottica 12
1.1.2. Funzionamento tecnico di trasmissione dei dati tramite i cavi sottomarini 17
1.2 L'INFRASTRUTTURA DEI CAVI SOTTOMARINI **18**
1.3 BREVE STORIA DEI CAVI SOTTOMARINI **21**
1.3.1 Era del Telegrafo 21
1.3.2 Era telefonica 24
1.3.3 Era della fibra ottica 25
1.3.4. Sviluppi tecnologici 26
1.4 PROFILI DI CARATTERE TECNICO E FUNZIONALE **28**
1.4.1 Come vengono posati i cavi sottomarini 28
1.3.2 Come vengono riparati i cavi 30
1.5 I SETTORI COINVOLTI **32**
1.5.1 Il rischio per il sistema finanziario 32
1.5.2 Impatto sul settore militare 34
CAPITOLO 2 ..... *36*
IL REGIME GIURIDICO DEI CAVI SOTTOMARINI *36*
2.0 INTRODUZIONE **36**
2.1 L'INSTALLAZIONE DEI CAVI SOTTOMARINI **39**
2.1.1 Alto mare 39
2.1.2 La Zona Economica Esclusiva e la Piattaforma Continentale 40
2.1.3 Acque Territoriali 41
2.2 LA PROTEZIONE DEI CAVI SOTTOMARINI **41**
2.2.1 Acque territoriali 41
2.2.2 Acque Internazionali, Zona Economica Esclusiva e Piattaforma Continentale 41
2.3. DANNI AI CAVI SOTTOMARINI: LE RESPONSABILITA' DEGLI STATI IN TEMPO DI PACE **43**
2.3.1 Responsabilità dello stato per danni accidentali ai cavi 44
2.3.2 Danni statali o supportati dallo stato ai cavi sottomarini 45
2.3.3 Gli attacchi cibernetici 45
2.3.4 Il taglio di un cavo sottomarino e il diritto dei conflitti armati 48

2.4 SOGGETTI PUBBLICI E PRIVATI 51
2.4.1 Modelli Commerciali 52
2.4.2 Metodi di finanziamento 53
2.4.3 Tipologie di aziende 54
2.5 LE TENDENZE DEL MERCATO 56
2.6 ORGANIZZAZIONI INTERNAZIONALI E UNIONE EUROPEA: LA GOVERNANCE GLOBALE DEI CAVI SOTTOMARINI 59
2.6.1 Organizzazioni Internazionali 59
2.6.2 Il Comitato Internazionale per la Protezione dei Cavi Sottomarini 60
2.6.3 UNIONE EUROPEA 61
2.6.4. Sicurezza Marittima e Cyber Security 62
2.6.5 Gli altri campi di intervento: governance marittima, politica digitale e infrastrutture, politica estera. 63
2.6.6 Stati Membri 64
CAPITOLO 3 66
3.0 I RISCHI E LA PROTEZIONE DEI CAVI SOTTOMARINI 66
3.1 DANNI ACCIDENTALI 68
3.1.1 Danni naturali 69
3.1.2 Danni fisici 70
3.2 DANNI INTENZIONALI 71
3.2.1 Analisi delle minacce provenienti da attori non statali 71
3.2.2 Le minacce provenienti da attori statali: il caso della Russia e della Cina 74
3.2.2.1 LA RUSSIA 74
3.2.4 Altre tipologie di attacco deliberato: gli attacchi digitali e le minacce al Network Management Systems 78
3.3 ATTIVITA' DI INTELLIGENCE E CAVI SOTTOMARINI 81
3.4 LE FRAGILITA' INFRASTRUTTURALI DEI CAVI SOTTOMARINI 85
3.5 IMPATTO DELLE MINACCE E MITIGAZIONE DEL RISCHIO 92
3.5.1 Mitigazione del rischio 93
CAPITOLO 4 95
LA GEOPOLITICA DEI CAVI SOTTOMARINI 95
4.1 LA POTENZA COMMERCIALE CINESE 97
4.1.1 Digital Silk Road 98
4.1.2 Il cavo PEACE ed il Progetto Cina-Pakistan in Fibra Ottica (CPFOP) 98
4.1.3 L'espansionismo cinese nel Mar Cinese Meridionale 102
4.1.4 Rimodellare internet tramite le aziende: la strategia cinese e russa 103
4.2 LA RUSSIA 105
4.2.1 Organizzazione interna: l'intelligence dei fondali marini 107
4.2.2 Gli assetti della Marina Militare Russa 110

4.2.3 I Cavi Sottomarini Danneggiati in Norvegia 114
4.3 STATI UNITI 115
4.3.1 Il quadro giuridico degli Stati Uniti e le sue risposte politiche 115
4.3.2 La guerra fredda dei cavi sottomarini tra Stati Uniti e Cina 118
4.3.3 L'iniziativa Clean Network 121
CAPITOLO 5 123
Infrastrutture critiche e sicurezza nazionale: il ruolo dei cavi sottomarini per l'Europa e l'Italia 123
5.1 L'APPROCCIO ITALIANO AL DOMINIO SUBACQUEO 123
5.1.1 Polo di Innovazione Nazionale per il Subacqueo 124
5.1.2 Risorse e strategie della Marina Militare Italiana per l'Underwater ed i cavi sottomarini 125
5.2 LE CRITICITA' ED I PUNTI DI FORZA DEI CAVI SOTTOMARINI ITALIANI 128
5.2.1 Progetti Futuri 130
5.3 SPIONAGGIO SOTTOMARINO: LE OPERAZIONI TEMPORA E PRISMA 132
5.3.1 Le fragilità dei punti di approdo nel Mediterraneo 134
5.4 CAVI SOTTOMARINI E INFRASTRUTTURE CRITICHE: LA LEGISLAZIONE EUROPEA E NAZIONALE 135
5.4.1 L'evoluzione della Strategia Europea in materia di Cybersicurezza 136
5.4.2 Codice Europeo delle Comunicazioni Elettroniche (EECC) 138
5.4.3 Strategia Europea in materia di Cybersicurezza 2020 140
5.4.4. LA Direttiva NIS 1 141
5.4.5 La revisione della Direttiva NIS e la Direttiva sulla Resilienza dei Soggetti Critici 142
5.5. LA LEGISLAZIONE NAZIONALE 144
5.5.1 Perimetro di Sicurezza Nazionale Cibernetica 144
5.5.2 Il Golden Power ed il caso Sparkle 146
CONCLUSIONI 151
Riferimenti 155

I CAVI SOTTOMARINI. DATI E INFRASTRUTTURE PER LE COMUNICAZIONI E LA DIFESA

INTRODUZIONE

"Today, the cyber economy is the economy. . . . Corrupt those networks and you disrupt this nation"

Condoleeza Rice – Segretaria di Stato degli Stati Uniti[1]

È notte fonda e una giovane coppia è di ritorno dal loro primo viaggio post Pandemia. Poche ore e atterreranno a New York in tempo per poter assistere al Super Bowl insieme agli amici di una vita. Insieme a loro vi saranno 100 milioni di telespettatori da tutto il mondo. All'improvviso il silenzio. Tutto tace. Cellulari, Televisioni. Niente tweet o storie Instagram. Un blackout generale che spaventa e isola tutto il mondo. Semplicemente Internet si è spento. Questo è l'inizio dello splendido libro "Silenzio" di Don Delillo che si interroga su quale sarebbe la reazione dell'essere umano ad una simile catastrofe[2]. Uno scenario apocalittico che in realtà è molto meno surreale di quanto si possa pensare. Un contesto in cui gli abitanti dell'isola di Tonga si sono ritrovati in seguito all'eruzione del vulcano Hunga Tonga–Hunga Ha'apai avvenuta il 15 gennaio 2022 che aveva distrutto l'unico cavo sottomarino per le comunicazioni che unisce Tonga con le isole Fiji[3]. Per ristabilire le comunicazioni ci sono volute più di tre settimane con un costo, per la sola riparazione del cavo, di oltre 200.000 dollari. Un evento del genere sarebbe in grado di paralizzare la vita economica e sociale di un paese. La dipendenza delle nostre società da Internet è aumentata notevolmente con la pandemia del Covid-19 durante la quale aziende e cittadini hanno dovuto digitalizzare gran parte delle loro attività. La quantità di dati che transitano sui cavi sottomarini è destinata ad aumentare a causa dell'introduzione del 5G ed al sempre più frequente ricorso al cloud computing da parte delle aziende[4]. Basti pensare che nel 2023, gli utenti globali, che ad oggi sono il 64% della popolazione mondiale, hanno utilizzato

[1] United States Congress – Joint Economic Committee, Security in the Information Age: New Challenges, New Strategies, 1 maggio 2001. Accessibile a https://www.jec.senate.gov/public/index.cfm/republicans/2002/5/security-in-the-information-age-new-challenges-new-strategies_1172.
[2] Don DeLillo, Il silenzio, Einaudi, 2021, pp.112.
[3] L. Bignami, Tonga è isolata dal resto del mondo. Colpa di un cavo rotto, Focus, 24 gennaio 2022. Accessibile a https://www.focus.it/scienza/scienze/vulcano-internet-tonga-isolata#:~:text=Non%20%C3%A8%20la%20prima%20volta,sopra%20il%20cavo%2C%20danneggiandolo%20gravemente.
[4] J. Sherman and Tinajiu Zuo, Cloud Computing As Critical Infrastructure, Atlantic Council, non ancora pubblicato.

Internet con una media di 6 ore al giorno[5]. Oggigiorno, la maggior parte dei nostri dati sono salvati sul cloud e non sulle memorie interne ai nostri computer. Ciò è sicuramente più funzionale alle nostre esigenze ma allo stesso tempo rende i dati più vulnerabili da attacchi esterni. Il rapporto che intercorre tra la crescita di banda larga, l'utilizzo dei cloud services ed i cavi sottomarini è dimostrato dall'ingresso di hyper-scalers[6] come Amazon, Google e Microsoft in questo mercato. Fino a pochi anni fa queste aziende compravano dalle compagnie telefoniche la disponibilità di banda larga sui cavi sottomarini mentre oggi sono loro stesse a possedere l'infrastruttura[7]. Si pensi che Microsoft, Google, Amazon e Meta oggi possiedono il 69% della capacità globale di trasmissione[8] ed utilizzano 2/3 della banda larga disponibile a livello globale.

L'ingresso di queste aziende ha avuto importanti conseguenze anche sulla morfologia di Internet. Se i dati sono l'oro del XXI secolo, ne consegue che le rotte su cui viaggiano siano similari a quelle commerciali. Storicamente, lo scopo delle compagnie telefoniche è stato quello di unire le principali città dove il traffico dati è maggiore. Tuttavia, le aziende sopracitate utilizzano i cavi per i loro servizi e il loro scopo è quello di unire i data center in giro per il mondo. La rotta più competitiva rimane quella che unisce Londra a New York ma si assiste alla nascita di rotte inedite da Virginia Beach alla Francia o dal Brasile all'Africa. Questo si lega alla crescita esponenziale nella domanda che sta vivendo sia il continente africano, dove pur vivendo il 17% della popolazione mondiale vi si trova solo l'1% dei data center globali, sia il Sud America.

Pertanto, i dati non viaggiano nell'etere tramite connessioni wireless o tramite satellite ma necessitano di un'infrastruttura fisica capillare. Ad oggi, si contano 574 cavi (attivi o pianificati) in tutto il mondo per una lunghezza complessiva di 1,4 milioni di chilometri[9]. Per dare un'idea delle dimensioni di cui si parla, si tratta di quattro volte la distanza che intercorre tra la terra e la luna. È possibile immaginare i cavi come le vene per il nostro corpo. Al posto del sangue sono attraversati dai dati che sono la linfa vitale del nostro organismo socio-economico. Cavi e vene condividono anche l'elemento della fragilità. Essi fungono da "autostrade" sottomarine, trasportando segnali di comunicazione ad alta velocità o energia elettrica su lunghe distanze. Non sorprende che i cavi sottomarini in fibra ottica

[5] M. Starri, Digital 2023 – i Dati Globali (Digital 2023 Global Overview Report), We are social, 26 gennaio 2023. Accessibile a https://wearesocial.com/it/blog/2023/01/digital-2023-i-dati-globali/.
[6] Gli hyperscaler sono provider di servizi cloud di grandi dimensioni che forniscono servizi scalabili a livello enterprise, come quelli di computing e storage
[7] Submarine Telecoms Forum, Inc., Submarine Telecoms Industry Report: 2020/2021 Edition, 23 ottobre 2020. Accessibile a https://subtelforum.com/products/ submarine-telecoms-industry-report/.
[8] Sydney, Brooke, Pleasic, Securing Subsea Cable Critical Infrastructure, Holes in the Governing Legal Framework in the United States and Internationally, Seton Hall University, 2024
[9] TeleGeography, Submarine Cable Frequently Asked Questions, 2024. Accessibile a https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions#:~:text=How%20many%20cables%20are%20there,and%20older%20cables%20are%20decommissioned.

nascono e crescono in parallelo alla globalizzazione di cui costituiscono la base tecnologica. La globalizzazione si fonda sull'interconnessione della società che si manifesta sia a livello produttivo nella filiera moderna della creazione di valore sia nella distribuzione delle risorse economiche tramite il mercato finanziario. Questo sviluppo tecnologico ha reso la società più veloce e caratterizzata da un rischio maggiore[10]. Vi è infatti la necessità che le informazioni viaggino in modo sempre più rapido affinché la globalizzazione possa funzionare. In questo senso, i cavi sottomarini sono l'infrastruttura critica per antonomasia, tanto fragili quanto essenziali. Il 99% delle comunicazioni digitali passa attraverso questi cavi[11]. Essi sono utilizzati in un numero sempre maggiore di ambiti, da quello energetico a quello scientifico (per lo studio dei fondali e delle maree) per fare alcuni esempi[12]. La quasi totalità delle nostre attività quotidiane presuppone l'utilizzo di internet, dai pagamenti alla comunicazione, dal funzionamento dei mezzi di trasporto alla logistica.

L'impatto dei cavi sottomarini è evidente soprattutto nel settore economico-finanziario. Secondo le stime della Federal Reserve statunitense, ogni giorno circa 10.000 miliardi di dollari (circa quattro volte il PIL annuale del Regno Unito) vengono trasmessi attraverso i cavi sottomarini. Inoltre, la Society for Worldwide Interbank Financial Telecommunication (SWIFT), che fornisce il quadro internazionale per circa 11.000 istituzioni finanziarie per condurre una media di 15 milioni di transazioni al giorno, dipende interamente dai cavi sottomarini[13]. Come afferma Karl Rauscher (presidente emerito dell'Institute of Electrical and Electronics Engineers e autore di un importante rapporto sui rischi associati ai cavi sottomarini[14]): "L'impatto di un tale guasto sulla sicurezza internazionale e sulla stabilità economica potrebbe essere devastante... Non è chiaro se la civiltà possa riprendersi dal fallimento di una tecnologia che è stata adottata così rapidamente senza un piano di riserva... Senza (la rete), il mercato economico-finanziario mondiale si bloccherebbe immediatamente".

Obiettivi e rilevanza della ricerca

Negli ultimi cinque-dieci anni, i principali attori internazionali come Stati Uniti, Cina e Russia, ma anche le grandi aziende tecnologiche, hanno prestato crescente attenzione all'importanza strategica della rete di cavi sottomarini nell'attuale competizione digitale. I cavi sottomarini rappresentano ora

[10] Raffaele Alberto Ventura, Radical Choc- ascesa e caduta dei competenti, Einaudi, 2020, pp.248.
[11] Jill C. Gallagher, Undersea Telecommunication Cables: Technology Overview and Issues for Congress, Congressional Research Service, 2022, pp 1-2.
[12] C. Manoj et al. , "Can undersea voltage measurements detect Tsunamis?" (2006) Earth Planets Space 58, 1–11; R. m onastersky, "The Next Wave" 2012 Nature 483, 144–146
[13] Rishi Sunak, Undersea Cables: Indispensable, Insicure, Policy Exchange, 2017.
[14] Karl Frederick Rauscher, ROGUCCI - The Report, Proceedings of the Reliability of Global Undersea Cable Communications Infrastructure Study & Global Summit, IEEE Communications Society, 2010. **Specificata fonte non valida.**

un nuovo importante campo di battaglia tecnologico per le potenze globali del mondo e dovrebbero essere trattati come una questione chiave negli studi sulla sicurezza, nella geopolitica e nell'analisi dei conflitti. Ciononostante, il tema suscita un basso interesse sia tra i policy maker che in ambito accademico. Secondo Bueger e Liebetrau, il motivo per cui i cavi non hanno assunto rilievo nel dibattito pubblico è riconducibile ad una "triplice invisibilità"[15]. La prima accomuna tutte le infrastrutture e consiste nel fatto che esse "risiedono in uno sfondo naturalizzato" e quindi i cittadini tendono a darle per scontate nonostante il ruolo che ricoprono[16]. In secondo luogo, quanto detto è ancor più accentuato nel caso dei cavi in quanto essi non sono visibili, a differenza dei ponti e delle strade che vengono utilizzati quotidianamente e possono anche essere fonte di controversia pubblica. I guasti ai cavi sottomarini sono rari e difficilmente la popolazione ne viene a conoscenza[17]. Infine, i cavi sottomarini sono situati nei fondali marini che sono uno dei luoghi meno conosciuti e visitati dall'uomo. Questo è anche uno dei motivi per cui il mare è stato sempre inteso come un ambiente che non necessitasse di regole in quanto privo di una vera e propria attività umana ma come un luogo di mero passaggio. Questo fenomeno è stato definito come "cecità del mare" e solo negli ultimi anni gli studi sulla sicurezza si stanno concentrando su questo nuovo dominio[18].

La crescita di questi studi si deve al cambio di paradigma geopolitico che ha interessato i concetti di terra e mare. In epoca moderna, i due ambienti sono stati trattati in modo fortemente distinto. La terra era il luogo dove gli stati avevano il loro centro di potere e sul quale proiettavano la propria forza. Queste dinamiche fanno parte della cosiddetta territorializzazione del mare[19] che si concretizza con la progressiva appropriazione, divisione e produzione degli spazi marittimi. È proprio quest'ultimo elemento che più rileva per tale studio. La globalizzazione ha da una parte eroso il potere dello stato sulla terraferma rendendolo dipendente da forze e dinamiche esterne ma allo stesso tempo gli ha consentito di acquisire un potere mai avuto nei confronti dell'ambiente marittimo in termini di conoscenza e di espansione della propria presenza fisica, specialmente in termini militari. Questo fenomeno sta trasformando le potenze talassocratiche in potenze "anfibie" che utilizzano il mare come piattaforma da cui sferrare attacchi militari o dove costruire infrastrutture critiche. I cavi sottomarini sono una perfetta rappresentazione di questa trasformazione geopolitica: un'infrastruttura

[15] Christian Bueger & Tobias Liebetrau (2021) Protecting hidden infrastructure: The security politics of the global submarine data cable network, Contemporary Security Policy, 42:3, 391-413.
[16] Edwards, P. N. Infrastructure and modernity: Force, time, and social organization in the history of sociotechnical systems. In P. Brey, A. Rip, & A. Feenberg (Eds.), *Technology and modernity: The empirical turn* (pp. 185–226). The MIT Press. 2013.
[17] N. Starosielski. 'Warning: Do not dig': Negotiating the visibility of critical infrastructures. *Journal of Visual Culture*, *11*(1), 38–57, 2012. Accessibile a https://doi.org/10.1177/1470412911430465
[18] Beyond seablindness: A new agenda for maritime security studies. *International Affairs*, *93*(6), 1293–1311.
[19] G. De Ruvo, Cosa sono le Zone Economiche Esclusive e come i Paesi si stanno spartendo i confini del mare, GeoPop, 10 gennaio 2023. Accessibile a https://www.geopop.it/zone-economiche-esclusive-cosa-sono-significato/

fisica che nasce sulla terra ma che continua sul mare e che necessita di essere protetta per poter garantire la sicurezza ed il funzionamento dei centri di potere situati sulla terraferma.

La ricerca sui cavi sottomarini si caratterizza per un approccio particolarmente settoriale in cui emergono tre approcci. In primis quello relativo alla vulnerabilità dei cavi sottomarini derivante da attacchi deliberati, soprattutto in relazione al diffondersi della guerra ibrida[20]. Un secondo ambito di studi si sofferma principalmente sulle problematiche tecniche che contraddistinguono i cavi sottomarini ed i possibili danni accidentali o non umani come le catastrofi naturali che avvengono nell'ambiente marittimo[21]. Infine, vi sono numerosi studi che trattano la tematica dal punto di vista normativo. In special modo, l'analisi si concentra sulle lacune e limitazioni del diritto Internazionale e sulle difficoltà derivanti dalla mancanza di una governance chiara dei cavi sottomarini.[22] Tuttavia, manca un approccio olistico alla materia che consenta di analizzare il ruolo dei cavi sottomarini alla luce delle attuali dinamiche geopolitiche. Le macroaree citate (sicurezza, tecnica e normativa) non possono essere osservate in modo distinto l'une dalle altre ma compongono un quadro articolato all'interno del quale si muovono gli attori privati e statuali. Un approccio settoriale risulta deficitario anche nel conferire le adeguate risposte. Infine, si sottolinea l'assenza di ricerche che si soffermino sul ruolo dell'Italia in questo contesto. Si riscontra una grande attenzione nei confronti degli attori dominanti ma il nostro paese risulta escluso da adeguate osservazioni circa i suoi interessi e le minacce per la sicurezza nazionale che ne possono conseguire. Ciò sorprende vista la posizione geografica occupata dall'Italia.

Alla luce di quanto detto, il lavoro in questione si propone un duplice scopo. Innanzitutto, quello di trattare i cavi sottomarini a 360 gradi. Lo scopo è quello di raccogliere in un unico documento la quasi totalità dei temi di rilievo per i cavi sottomarini. L'ambizione è quella di poter rappresentare una fonte bibliografica di riferimento per i futuri ricercatori che, indipendentemente dallo specifico ambito che vorranno indagare, troveranno informazioni utili all'interno di quest'opera. Quindi, da una parte il taglio stilistico è simile a quello della manualistica in modo tale da poter essere un punto di riferimento anche per coloro i quali si avvicinano a questo mondo per la prima volta. Per questa

[20] Vedi soprattutto Sechrist, M. (2012). *New threats, old technology: Vulnerabilities in undersea communications cable network management system*. Harvard Kennedy School, Belfer Center for International Affairs¸ Ross, M. (2014). Understanding interconnectivity of the global undersea cable communications infrastructure and Its implications for international cyber security. *SAIS Review of International Affairs*, *34*(1), 141–155. Martinage, R. (2015). Under the sea. The vulnerability of the commons. *Foreign Affairs*, *94*(1), 117–122.

[21] Pope, E. L., Talling, P. J., & Carter, L. Which earthquakes trigger damaging submarine mass movements: Insights from a global record of submarine cable breaks? *Marine Geology*, *384*, 2017, 131–14; Schaub, Jr., G., Murphy, J. M., & Hoffman, F. (2017). Hybrid maritime warfare: Building baltic resilience. *The RUSI Journal*, *162*(1), 32–40.

[22] Burnett, D. R., Beckman, R. & Davenport, T. M. (Eds.). (2013) *Submarine cables: The Handbook of Law and policy*. Brill; Davenport, T. M. (2015). Submarine cables, cybersecurity and international law: An intersectional analysis. *Catholic University Journal of Law and Technology*, *24*(1), 57–104

ragione, l'ordine dei capitoli e dei paragrafi segue un iter logico ben preciso. L'obiettivo è quello di fornire passo dopo passo nozioni propedeutiche all'analisi del paragrafo successivo con una logica simile a quella dei puzzle. Man mano che si procederà nella lettura e si inseriranno le varie tessere, sarà sempre più chiaro il disegno completo e la tesi che si vuole dimostrare con questo elaborato.

Un'infrastruttura che si estende per 1.4 milioni di chilometri, che si posa sui fondali dell'oceano e che misura poco più di un tubo da giardino, presenta delle caratteristiche tecniche altamente complesse. Sono queste caratteristiche che determinano che tipi di minacce devono affrontare i cavi sottomarini, le difficoltà nel normare il settore, il funzionamento del mercato e le posture assunte dagli stati nazionali. Pertanto, il primo capitolo si focalizza su cosa sia un cavo sottomarino, l'evoluzione storica di questa infrastruttura, il processo di installazione e posa del cavo per terminare con un'analisi dell'impatto dei cavi sottomarini nei diversi settori ed in special modo in quella della difesa. Compreso il funzionamento tecnico dell'infrastruttura, nel secondo capitolo si tratta la legislazione internazionale, in tempo di pace e di guerra, ed il ruolo ricoperto dai privati che sono gli attori principali. Compresa la legislazione inerente i cavi sottomarini si passa ad analizzare la governance europea ed internazionale che risulterà centrale nel capitolo conclusivo. Il terzo capitolo si sofferma sulle minacce fisiche e digitali, umane ed accidentali, proprie di questa infrastruttura. In questo capitolo il lato tecnico descritto ad inizio lavoro si mischia con elementi propri della geopolitica e degli studi sulla sicurezza. Il quarto capitolo è prettamente di natura geopolitica e studia le politiche e strategie adottate dalle tre grandi superpotenze: la Cina con il suo espansionismo commerciale, la Russia con il suo approccio militarista e la potenza egemone degli Stati Uniti. Anche in questo caso, il capitolo è comprensibile solo alla luce delle analisi che lo precedono ma è allo stesso tempo propedeutico per il capitolo conclusivo nel quale si analizzano i cavi sottomarini sia come infrastruttura critica che per il ruolo che hanno nella sicurezza nazionale.

Infine, nel capitolo conclusivo di evidenzierà la maggiore criticità dei cavi sottomarini su cui, a mio avviso, bisognerà intervenire: i cavi sottomarini sono un'infrastruttura critica che rende i paesi dipendenti gli uni dagli altri e ciò rende i cavi oggetto delle politiche europee. Allo stesso tempo, i cavi sono un'infrastruttura cruciale per la sicurezza nazionale dei singoli paesi in quanto possono essere utilizzati sia come vettori per attacchi digitali sia per operazioni di spionaggio. Il problema risiede nel fatto che la sicurezza nazionale è una materia su cui i paesi sono particolarmente gelosi e non vogliono cedere sovranità nei confronti dell'Europa. Si cercherà di dimostrare come questa sia la ragione per cui fino ad oggi non si sia elaborata un'appropriata governance in materia di cavi sottomarini e via sia l'assenza di una strategia europea in merito. Alla fine di questa ricerca sarà evidente come le soluzioni nazionali siano insufficienti a mitigare minacce di natura globale e sia

necessario un approccio interdisciplinare e sovranazionale affinché l'Europa ricopra un ruolo chiave nella sicurezza delle informazioni e nella protezione dei suoi cittadini.

CAPITOLO 1
CAVI E DATI

1.1 NOZIONI E TIPOLOGIE

In questo capitolo si vuole dare una panoramica dell'infrastruttura in cui si inseriscono i cavi e della sua complessità. Ognuno di questi paragrafi sarà propedeutico alla comprensione dei capitoli successivi. Si partirà dalla prima tessera del puzzle, il cavo stesso. Ne verrà analizzata la struttura e successivamente si allargherà lo sguardo a tutti gli elementi che ne permettono il funzionamento (landing station, IoP ecc). Questo risulterà cruciale per l'analisi dei rischi e delle possibili misure di protezione che si affronteranno nel terzo capitolo. Quindi si passerà a raccontare la storia dei cavi con un particolare accento sugli uomini e le aziende che hanno reso possibile tutto ciò. Difatti i cavi sottomarini sono un settore di rilevanza globale ma in cui i principali attori sono proprio i privati, come si vedrà nel secondo capitolo. Inoltre, sarà posta una particolare attenzione alle modalità di posa dei cavi sottomarini. In questo modo si potranno capire gli obblighi delle aziende, il difficile rapporto che vi intercorre con gli stati e soprattutto il potenziale impatto ambientale. Ciò sarà analizzato più nel dettaglio nel capitolo successivo. Infine, si analizzerà l'impatto che i cavi possono avere in diversi settori nevralgici come quello militare ed economico.

I cavi sottomarini si caratterizzano (e si differenziano) per la presenza di determinati elementi che analizzeremo nel dettaglio nel corso di questo capitolo. Come ci dice il nome stesso, l'elemento che più caratterizza il cavo sottomarino è l'ambiente nel quale si trova ad operare, quello subacqueo. Questo contesto pone numerose sfide per via dei fenomeni naturali che lo riguardano (terremoti, tsunami ecc.), della protezione di cui necessita e della poca conoscenza dei fondali marini da parte dell'uomo. Pertanto, il cavo si caratterizza innanzitutto per essere composto da elementi che gli permettono di operare in tali circostanze: una fibra che garantisca una bassa perdita di dati, una forte affidabilità e resistenza alla pressione (provocata dall'acqua) e alla tensione che gli permettano di funzionare per almeno 25 anni[23].

A livello internazionale non vi è una definizione univoca di "cavo sottomarino". L'International Telecommunication Union (ITU) definisce i cavi in diversi modi: "Il cavo sottomarino che utilizza le

[23] Wei Jiang, Submarine Optical Cable Engineering, Academic Press, 2018, pp. 9-10.

fibre ottiche come linea di trasmissione", oppure ""il cavo ottico sottomarino è un cavo in fibra ottica sottomarino progettato per essere adatto all'uso in acque basse e profonde, che deve garantire la protezione delle fibre ottiche dalla pressione dell'acqua, la propagazione longitudinale dell'acqua, l'aggressione chimica e l'effetto dell'idrogeno per tutta la durata del cavo"[24]. Nelle definizioni citate sembrano essere esclusi i cavi per la trasmissione dell'elettricità e si fa esplicito riferimento al fatto che tali cavi siano posati sui fondali. La fonte di carattere legislativo principale è l'UNCLOS che tuttavia non presenta una definizione di cavo sottomarino. I singoli stati hanno adottato definizioni molto diverse tra loro e spesso non le rendono accessibili al pubblico rendendo la ricerca complicata[25]. Per quanto concerne le fonti scientifiche, una delle definizioni più completa è quella dello Science Dictionary secondo cui il cavo sottomarino è "Cavo a lunga distanza posato sul fondo del mare. Di forma coassiale, con ripetitori sottomarini a intervalli per amplificare i segnali. In acque poco profonde, con pericolo di ancore o di pesca a strascico, i cavi possono essere corazzati o addirittura interrati nel fondale marino. In acque profonde, sono utilizzati cavi leggeri senza armatura, ma con un'anima centrale di acciaio ad alta resistenza per evitare lo stiramento durante la posa. Alcuni possono contenere canali in fibra ottica"[26]. Una delle definizioni più interessanti per la sua capacità di tenere insieme le varie sfaccettature che contraddistinguono i cavi sottomarini è la seguente: "Il cavo sottomarino internazionale è un cavo sottomarino indipendentemente dal suo tipo, progettato per il funzionamento sul fondale marino, posato in aree marittime stabilite in conformità al diritto internazionale, allo scopo di trasmettere corrente elettrica e segnali di telecomunicazione"[27]. Tuttavia, come si è potuto osservare da questa breve disamina, non esiste una definizione univoca di cavo sottomarino. Soltanto tramite un'attenta analisi delle sue componenti fisiche e dei funzionamenti tecnici sarà possibile avere un quadro di quello che è il soggetto dell'elaborato.

1.1.1 Cavi energetici e cavi in fibra ottica

I cavi si dividono principalmente tra quelli energetici e quelli per le telecomunicazioni. I cavi energetici giocano un ruolo essenziale nelle nostre economie. Ad esempio, sono uno dei pochi mezzi tramite cui i paesi possono scambiare energia pulita e a basso costo. Il primo cavo di alimentazione sottomarino fu installato nel 1811 attraverso il fiume Isar in Baviera[28]. I criteri su cui si valuta un

[24] International Telecommunication Union, ITU-T G.972, Telecommunication Standardization Sector Of ITU (11/2016), Series G: Transmission Systems And Media, Digital Systems And Networks Digital Sections And Digital Line System – Optical Fibre Submarine Cable Systems Definition Of Terms Relevant To Optical Fibre Submarine Cable Systems, Recommendation ITU-T G.972, paragraphs 1019, available at https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-G.972- 200406-S!!PDF-E&type=items, last visited 01/09/2020.
[25] D. Shvets, The international legal regime of submarine cables: a global public interest regime, Universitat Pompeu Fabra, 2020, Barcellona, pp. 34.
[26] Science Dictionary, Free Online Science Dictionary, definition of a "submarine cable", 2017.
[27] Op. Cit, D. Shvets, The international legal regime of submarine cables: a global public interest regime, 2020, pp. 39.
[28] R. Kandiyoti, "Under the Sea", 4(14) Engineering & Technology, 2009, pp. 26.

cavo energetico sono: la profondità di posa, il volume di elettricità trasportabile, l'affidabilità del sistema e la lunghezza del cavo. Questi sono anche i driver dell'evoluzione tecnologica di questa tipologia di cavi. Le tendenze storiche indicano che i maggiori sviluppi tecnologici hanno riguardato la lunghezza dei cavi.

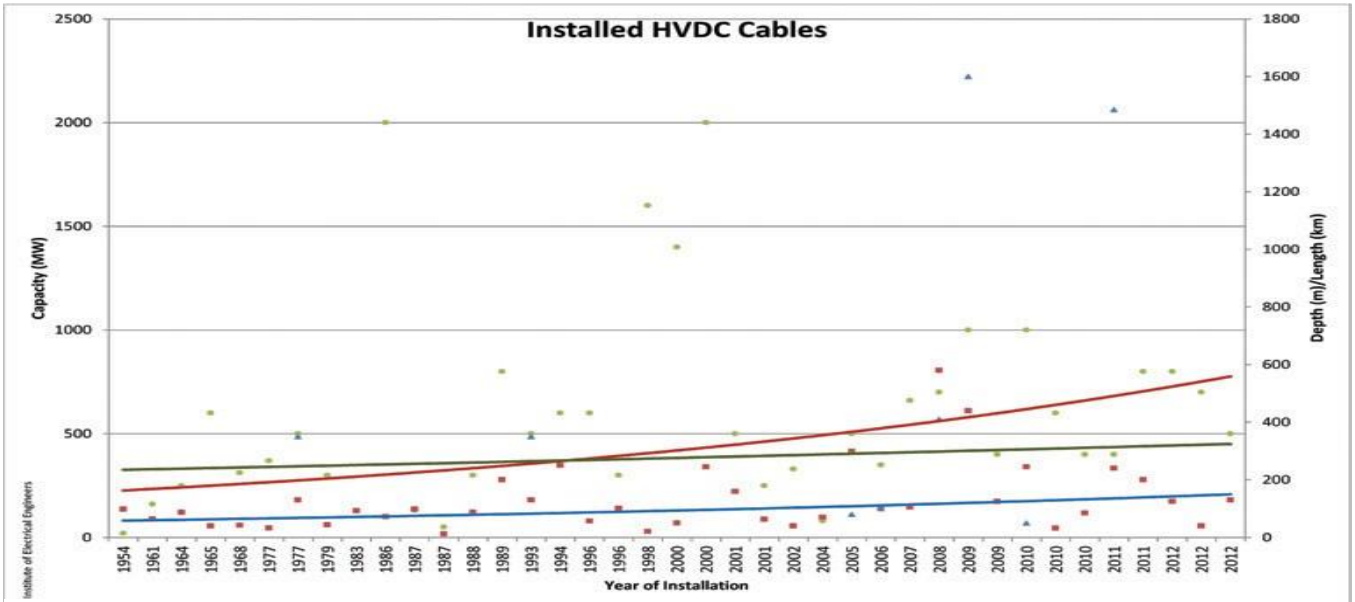


Figura 1: gura 1: sistemi di cavi ad alta tensione in corrente continua (HVDC) installati, con indicazione di profondità, lunghezza e capacità (Submarine Cables: D.R Bournett, R. B et al. Submarine Cables: The Handbook of Law and Policy. Martinus Nijhoff

I cavi si dividono principalmente tra quelli energetici e quelli per le telecomunicazioni. I cavi energetici giocano un ruolo essenziale nelle nostre economie. Ad esempio, sono uno dei pochi mezzi tramite cui i paesi possono scambiare energia pulita e a basso costo. Il primo cavo di alimentazione sottomarino fu installato nel 1811 attraverso il fiume Isar in Baviera[29]. I criteri su cui si valuta un cavo energetico sono: la profondità di posa, il volume di elettricità trasportabile, l'affidabilità del sistema e la lunghezza del cavo. Questi sono anche i driver dell'evoluzione tecnologica di questa tipologia di cavi. Le tendenze storiche indicano che i maggiori sviluppi tecnologici hanno riguardato la lunghezza dei cavi. Il primo cavo in corrente continua ad alta tensione (HVDC) Gotland 1 è stato installato nel 1954 a una distanza di 98km tra l'isola di Gotland e la terraferma svedese. Basti pensare che solamente 50 anni fa il cavo Basslink misurava una lunghezza di 298 km tra gli stati australiani di Tasmania e Victoria mentre oggi i cavi possono arrivare a misurare oltre 700 chilometri come nel caso del North Sea Link situato nel Mare del Nord che permetterà al Regno Unito di ridurre le sue

[29] R. Kandiyoti, "Under the Sea", 4(14) Engineering & Technology, 2009, pp. 26.

emissioni di carbonio di 23 milioni di tonnellate entro il 2030[30]. In territorio italiano si trova il cavo sottomarino energetico più profondo al mondo. Il SaPEI è stato posato nel 2008 ad una profondità di 1600 metri e collega la Sardegna alla penisola[31]. È bene ricordare che una delle principali sfide a cui sono sottoposti i cavi sottomarini è la pressione esercitata dall'acqua. A tali profondità risulta 160 volte maggiore rispetto a livello del mare. La pressione si ripercuote anche sui piani di manutenzione e riparazione. Difatti i cavi energetici possono arrivare a pesare tra i 50 e 70 kg al metro[32].

Esistono diverse tipologie di cavi energetici[33] ma i principali sono due e si basano su due sistemi di trasmissione distinti. Il primo sistema è quello in *corrente continua (*CC) così chiamato in quanto l'energia elettrica oscilla periodicamente e gradualmente tra polarità positive e negative mentre nel secondo sistema il flusso degli elettroni è unidirezionale. Il sistema predominante è quello della corrente alternata, utilizzato anche sulla terraferma nelle nostre case.

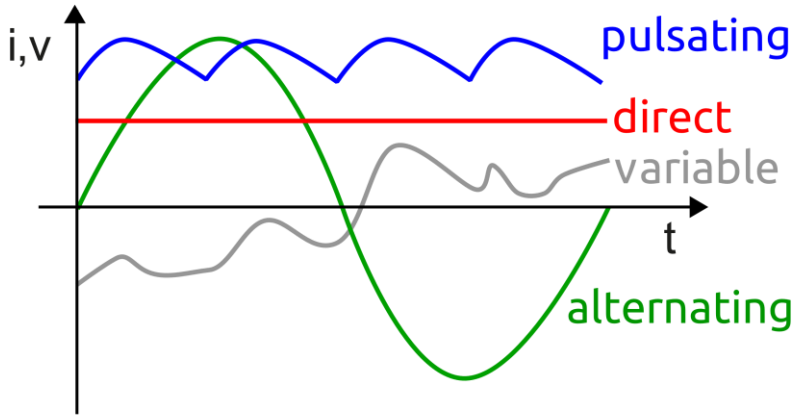


Figura 2: Corrente alternata (in verde). L'asse orizzontale misura il tempo; l'asse verticale misura la corrente o la tensione

Utilizzando una metafora, il sistema a Corrente Alternata può essere pensato come un'autostrada costruita per ospitare il traffico massimo che si verifica nelle ore di punta (i picchi delle onde sinusoidali) ma il resto del tempo è relativamente vuoto e non viene utilizzato (l'area grigia sotto la forma d'onda). La CC è la stessa autostrada ma il medesimo traffico viene distribuito in modo uniforme durante il giorno senza che vi siano dispersioni di energia. Per questo motivo i cavi in corrente alternata sono adatti a trasportare grandi quantità di potenza elettrica. I cavi in corrente continua, d'altra parte, sono comunemente utilizzati per collegamenti a lunga distanza tra reti di

[30] "Tra Gran Bretagna e Norvegia attivo il cavo elettrico sottomarino più lungo del mondo - The MediTelegraph", The Medi Telegraph, 2021.
[31] Ardelean, M., Minnebo, HVDC Submarine Power Cables in the World; 2015, doi: 10.2790/95735
[32] D.R Bournett, R. B et al. *Submarine Cables: The Handbook of Law and Policy,* Martinus Nijhoff, 2013.
[33] Oltre ai cavi in CC e CA esistono anche le seguenti tipologie: i cavi sottomarini per l'interconnessione di parchi eolici offshore, per l'interconnessione di piattaforme petrolifere, per l'interconnessione di sistemi di energia rinnovabile.

alimentazione e sistemi isolati in quanto presentano una minore perdita di energia nella trasmissione. Per le sue caratteristiche di trasmissione lineare a grande distanza, la corrente continua HVDC è trasmessa tramite linee aeree o cavi sottomarini. Lo svantaggio maggiore di questo tipo di tecnologia è che necessita di stazioni di conversione che risultano essere molto costose.[34] A differenza dei cavi in fibra ottica, unire un cavo in CA e uno in CC richiede costi molti alti e personale altamente qualificato. Questo fa sì che vi sia una bassa interoperabilità tra i diversi sistemi di cavi energetici con gravi ripercussioni sulla manutenzione e riparazione. Per abbassare i costi i privati cercano di convogliare il maggior numero possibile di cavi in stazioni di riconversione già esistenti in modo da non doverne costruire di nuove. Purtroppo, questa dinamica ha delle ripercussioni sulla sicurezza in quanto si diminuisce la ridondanza del sistema[35].

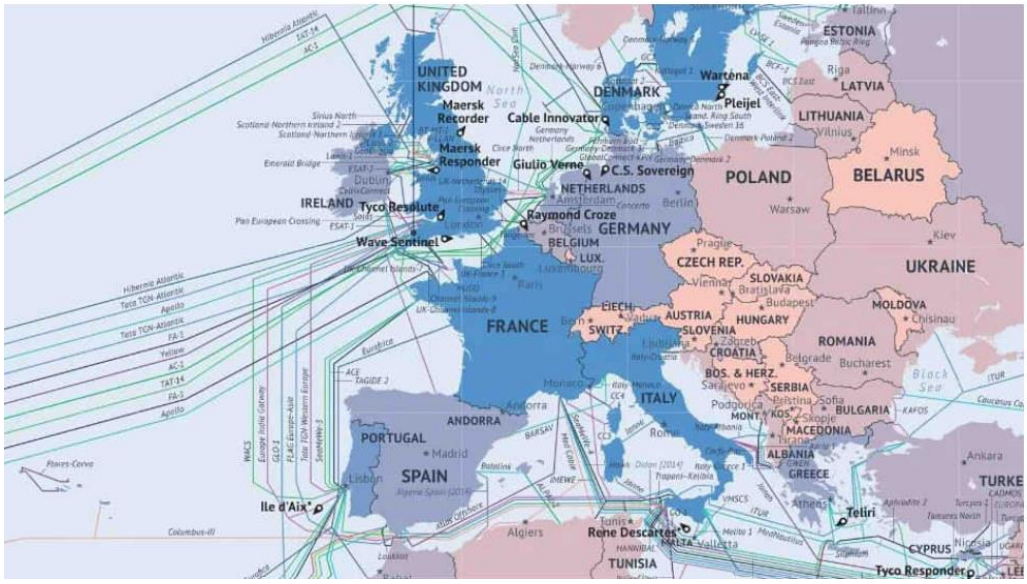


Figura 3: i cavi sottomarini in Europa. Fonte: Global Wind Report 2021, Global Wind Energy Council

I cavi energetici e per le telecomunicazioni presentano alcune differenze in termini strutturali che hanno delle ripercussioni non solo di natura tecnica ma anche su dove saranno posati i cavi e sui costi che ne conseguono. Difatti i cavi non sono sempre costruiti lungo la rotta più veloce tra due punti terrestri ma bisogna prendere in considerazione altri elementi come la topografia del terreno e dove si trovano le strutture più adatte a far atterrare il cavo. I conduttori utilizzati per i cavi sottomarini, energetici ed in fibra ottica, sono principalmente costituiti in fili di rame o alluminio ma le dimensioni sono molto diverse. D'altronde in un caso il cavo deve trasmettere corrente elettrica ad alta tensione

[34] Worzyk, T.: Submarine power cables: Design, installation, repair, environmental aspects. In: Submarine Power Cables: Design, Installation, Repair, Environmental Aspects, pp. 9–50. Springer Science & Business Media, Berlin-Heidelberg (2009)

[35] "La maggior parte delle aziende o Stati che utilizzano i cavi segue un approccio di "sicurezza nei numeri", distribuendo la capacità delle loro reti su più cavi in modo che se uno si interrompe, la loro rete funzionerà senza problemi su altri cavi mentre il servizio viene ripristinato su quello danneggiato. Questa è la ridondanza." P. Brodsky, Submarine Cable Redundancy, Explained, Accessed at https://blog.telegeography.com/what-is-submarine-cable-redundancy

(e necessiterà di maggiori protezioni e dimensioni) mentre i cavi per le telecomunicazioni trasmettono segnali elettrici ad alta frequenza. Per quanto concerne l'isolamento, i cavi energetici devono poter gestire elevate tensioni elettriche in un ambiente completamente marittimo mentre i cavi in fibra ottica devono essere protetti dall'interferenza elettromagnetica. Non bisogna dimenticare che viste le difficoltà nel riparare i cavi energetici, questi sono costruiti per avere una vita più lunga (tra i 40 e 65 anni[36]) di quelli per le telecomunicazioni.

I cavi in fibra ottica risultano particolarmente piccoli ma allo stesso tempo devono garantire un alto livello di protezione. Il Nucleo in fibra ottica è il componente principale del cavo sottomarino ed è costituito da una o più fibre ottiche. Le fibre ottiche sono fili sottili e trasparenti realizzati in vetro o plastica speciale. Queste fibre sono progettate per trasportare i segnali ottici che portano le informazioni attraverso la riflessione interna totale della luce. Poi vi è la guaina di protezione che avvolge il nucleo in fibra ottica per fornire isolamento e protezione meccanica. Lo Strato di rinforzo fornisce resistenza alla trazione e protezione contro la deformazione. Inoltre alcuni cavi sottomarini possono includere uno strato di schermatura per proteggere le fibre ottiche dalle interferenze elettromagnetiche esterne. Infine il cavo sottomarino può contenere un materiale di riempimento (come il gel o il politilene espanso) per proteggere il nucleo e fornire supporto strutturale.

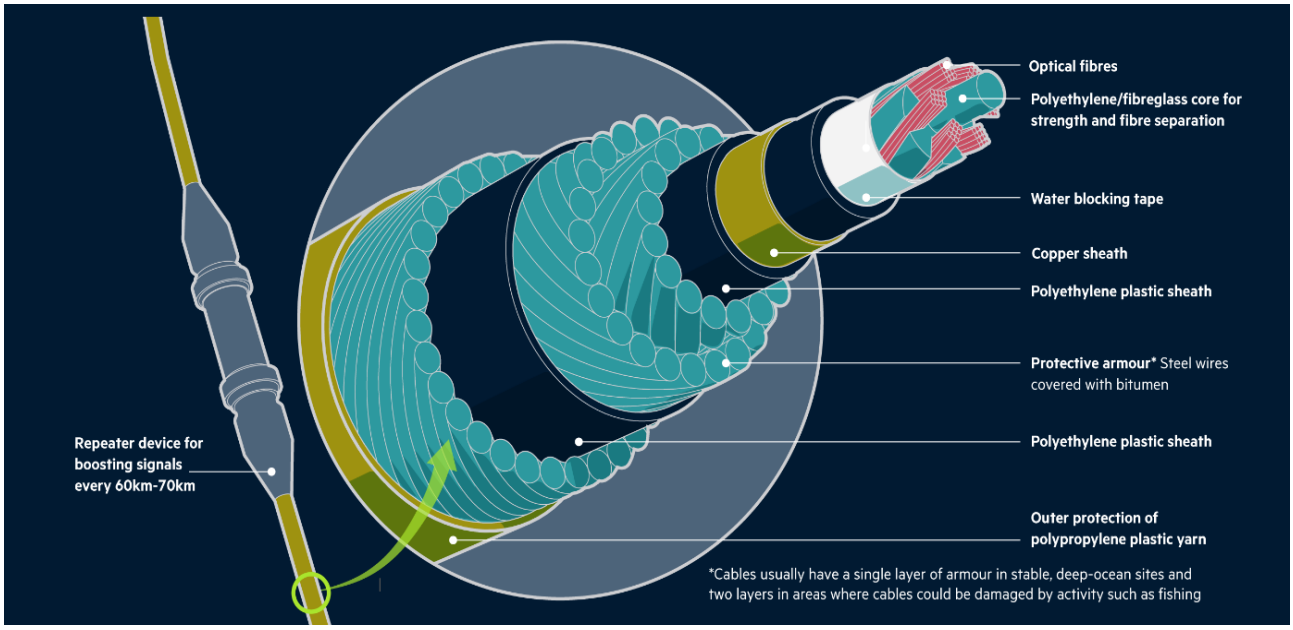


Figura 4: Anna Gross, Alexandra Heal, Chris Campbell, How the US is pushing China out of the internet's plumbing,Financial Times, 13 giugno 2023.

Dove i cavi si avvicinano alla riva e sono soggetti all'effetto del movimento in acqua è necessario proteggersi dal deterioramento e dalla corrosione proteggendo l'anima con un'armatura più pesante.

[36] Ivi. pp.340

Così i cavi variano in spessore da un pollice di diametro (cavo di acque profonde) del peso di circa 2,5 tonnellate per miglio, a quattro pollici e mezzo di diametro (cavo all'estremità della costa) del peso di circa 60 tonnellate per miglio.

1.1.2. Funzionamento tecnico di trasmissione dei dati tramite i cavi sottomarini

Ogni giorno ci scambiamo messaggi o foto alla rapidità della luce. Questo scambio di informazioni è possibile grazie a diversi strumenti e procedimenti tecnici molto complicati. Alla base di questo processo vi è il fascio di luce veicolato tramite la fibra ottica. La luce non ha alcun problema a percorrere enormi distanze in linea retta, per esempio attraverso un lunghissimo corridoio. Tuttavia i cavi hanno percorsi tortuosi e con molte curve in quanto devono seguire l'andamento dei fondali marini. Pertanto, se si vuole far arrivare il fascio di luce alla fine del percorso è necessario posizionare su ciascuna curva degli "specchi" su cui far rimbalzare la luce. Questa è la semplificazione di un fenomeno ben più complesso definito "riflessione interna totale": poiché il rivestimento non assorbe luce dal nucleo, l'onda luminosa può percorrere grandi distanze rimbalzando sulle pareti del cavo. Ciononostante, parte del segnale all'interno della fibra viene perso mentre percorre distanze maggiori. L'entità della degradazione del segnale dipende dalla purezza del vetro, dal numero di curve nella fibra o giunzioni che collegano sezioni di fibra e dalla lunghezza d'onda della luce trasmessa.

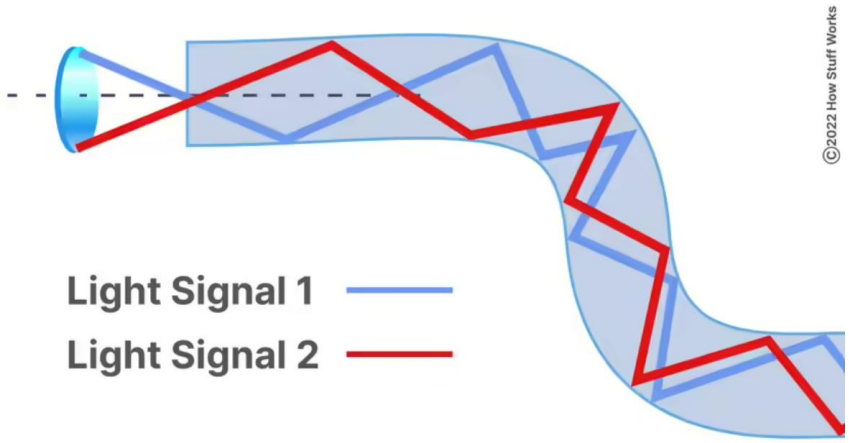


Figura 5: Diagramma della riflessione interna totale in una fibra ottica

FONTE: ONLINE2DESIGN.COM/HOWSTUFFWORKS

Sempre utilizzando una metafora è possibile paragonare la comunicazione tramite fibra a quella che veniva eseguita dai marinai durante la Seconda guerra mondiale usando il codice MORSE. Il marinaio riceveva il messaggio dal capitano, lo traduceva in codice Morse (una sequenza di punti e tratti) e lo riproduceva tramite un'apposita luce di segnalazione. Un altro marinaio, posizionato su una nave dinnanzi a lui, lo vedeva e decodificava dal linguaggio Morse. Il meccanismo è simile ma cambiano gli strumenti utilizzati per riprodurre il fascio di luce e per decodificare il messaggio. Innanzitutto i

dati(immagini, testo, video ecc) devono essere convertiti in segnali elettrici che a loro volta dovranno trasformarsi in segnali ottici. Qui interviene il trasmettitore in modo analogo al marinaio della nave mittente. Il trasmettitore riceve e dirige il dispositivo ottico per "accendere" e "spegnere" la luce nella sequenza corretta, generando così un segnale luminoso. Il trasmettitore è fisicamente vicino alla fibra ottica e può anche avere una lente per focalizzare la luce nella fibra. I laser hanno più potenza dei LED e sono utilizzati per trasmettere informazioni su lunghe distanze ma sono anche notevolmente più costosi dei LED. Durante il percorso attraverso il cavo sottomarino, il segnale ottico può perdere intensità a causa dell'attenuazione. Per mantenere il segnale forte e leggibile, vengono utilizzati amplificatori ottici, come gli amplificatori a fibra ottica erbium-doped (EDFA), per amplificare il segnale lungo il percorso[37]. Alla fine del cavo sottomarino, il segnale ottico viene ricevuto da un dispositivo chiamato "ricevitore ottico". Esso è come il marinaio sul ponte della nave ricevente. Prende i segnali luminosi digitali in arrivo, li decodifica e invia il segnale elettrico al computer, alla TV o al telefono dell'altro utente (che rappresenta il comandante della nave ricevente)[38]. I dati digitali giungono sotto forma di una sequenza di 0 e 1 e, in modo analogo al codice Morse, verranno codificati dai processori dei nostri dispositivi, decriptati se necessario, e resi accessibili per gli utenti.

1.2 L'INFRASTRUTTURA DEI CAVI SOTTOMARINI

L'infrastruttura dei cavi sottomarini è un sistema altamente complesso e integrato. I cavi rappresentano solo un elemento ma non possono funzionare da soli. Il cavo sottomarino rappresenta il punto di giunzione tra le varie strutture terrestri tramite cui vengono gestite le nostre comunicazioni. Per comprendere le dinamiche legislative e geopolitiche che analizzeremo successivamente è importante aver presente l'intera struttura.

Come si è già anticipato, internet è tutt'altro che qualcosa di etereo e i dati non si muovono in modo astratto tramite l'aria come dei piccioni viaggiatori. Alla base delle nostre comunicazioni vi è un'infrastruttura fisica molto pesante e capillare. La struttura di cui parliamo può essere suddivisa in tre sezioni: una parte chiamata *wet plant,* una *dry plant* e poi vi è la rete internet terrestre. Ripercorrendo il tragitto dei dati a partire dai nostri telefoni sarà tutto più chiaro.

[37] Un rigeneratore ottico è costituito da fibre ottiche con uno speciale rivestimento (drogaggio). La porzione drogata viene "pompata" con un laser . Quando il segnale degradato entra nel rivestimento drogato, l'energia del laser consente alle molecole drogate di diventare esse stesse laser . Le molecole drogate emettono quindi un nuovo segnale luminoso più forte con le stesse caratteristiche del debole segnale luminoso in arrivo. Fondamentalmente, il rigeneratore è un amplificatore laser per il segnale in ingresso.

[38] Il ricevitore utilizza una fotocellula o un fotodiodo per rilevare la luce. Infatti, quando gli impulsi luminosi arrivano al fotodiodo, la luce colpisce la sua superficie e crea una piccola corrente elettrica proporzionale all'intensità della luce. Successivamente, il circuito di conversione amplifica e converte questa corrente elettrica in un segnale elettrico più forte e adatto per l'elaborazione. Questo segnale elettrico può quindi essere inviato ai dispositivi che desideriamo utilizzare, come un computer o un telefono, dove verrà codificato.

Figura 6: Viavi Solutions, Submarine Cable Networks. Accessibile a https://www.viavisolutions.com/en-us/submarine-cable-networks

Quando avviamo una chiamata i nostri telefoni si connettono alla torre dati più vicina (tramite tecnologia wireless o fibra ottica[39]. Queste a loro volta veicolano il traffico dati ai cd. *Data centers e Point of Presence* tramite il sistema di backhaul. Nel contesto della rete Internet, il sistema backhaul è collegamento tra i nodi di accesso, come torri di trasmissione wireless o cabine di distribuzione di servizi Internet, e i punti centrali di aggregazione dei dati, come i data center o i Point of Presence (PoP). I primi sono strutture che hanno lo scopo principale di archiviare, gestire e rendere disponibili i dati inviati mentre i secondi sono il punto di ingresso e uscita delle comunicazioni internazionali e permettono il collegamento con gli altri operatori di rete, fornitori di servizi Internet, aziende e utenti finali. Queste strutture sono i punti di giunzione con la parte "secca" del sistema che si compone di almeno tre strutture: landing station, Beach Manhole e outside plant. E' tramite questa sezione che avviene il controllo sui dati che attraversano i cavi e sullo stato di quest'ultimi. Come verrà analizzato successivamente, alcune delle principali vulnerabilità del sistema sono legati proprio a questi edifici.

Il *Beach Manhole* è una camera di cemento, interrata nella spiaggia o nella strada dietro il punto di approdo (simile a un tombino), dove il cavo sottomarino termina e da cui il cavo in fibra e il cavo di alimentazione vengono indirizzati alla *Cable Landing Station (* CLS o "punti di approdo"). Inoltre, il Beach Manhole offre un punto di accesso per le operazioni di ispezione, manutenzione e riparazione del cavo sottomarino. La maggior parte dei pozzetti è progettata per accogliere più di un cavo, di solito due[40]. Inoltre, i punti di approdo possono vedere più pozzetti in prossimità l'uno dell'altro. Sebbene queste due situazioni siano economicamente vantaggiose, potrebbero aumentare il rischio di

[39] "Submarine Cable Frequently Asked Questions", TeleGeography, accessed at https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions
[40] CSRIC WG4A—Final Report on Cable Landings, p. 4.

guasti, in quanto un singolo evento localizzato potrebbe interrompere più cavi, ad esempio la distruzione dell'area a causa di un uragano o il danneggiamento di una ruspa su due cavi contemporaneamente[41].

La *Landing Stations* è un edificio che fornisce l'alimentazione (PFE) e le apparecchiature terminali delle linee sottomarine(SLTE). All'interno di una landing cable station, i cavi sottomarini vengono connessi ad apparecchiature di trasmissione e ricezione, come multiplexer, convertitori di segnale e attrezzature di routing[42]. Queste apparecchiature consentono la trasmissione e la ricezione dei segnali ottici o elettrici attraverso i cavi sottomarini. Inoltre, esse possono anche ospitare apparecchiature per il monitoraggio e la manutenzione dei cavi sottomarini, nonché personale specializzato per la gestione e la manutenzione delle connessioni dei cavi. Tuttavia, il controllo dello stato dei cavi viene sempre più effettuato a distanza tramite i Network Management System che sono degli appositi software. Sostanzialmente è da questi edifici che si controlla il traffico dei dati sottomarini. Queste strutture contengono anche i sistemi necessari per l'energia dei ripetitori di segnale contenuti nei cavi. Un CLS può essere un piccolo edificio in una piccola città costiera o parte di un centro dati molto più grande. In entrambi i casi, si tratta di strutture cruciali che necessiterebbero di molta sicurezza e riservatezza. Infine, per *Outside plant* si intendono i condotti, i cavi in fibra e i cavi di alimentazione tra il BMH e il CLS.

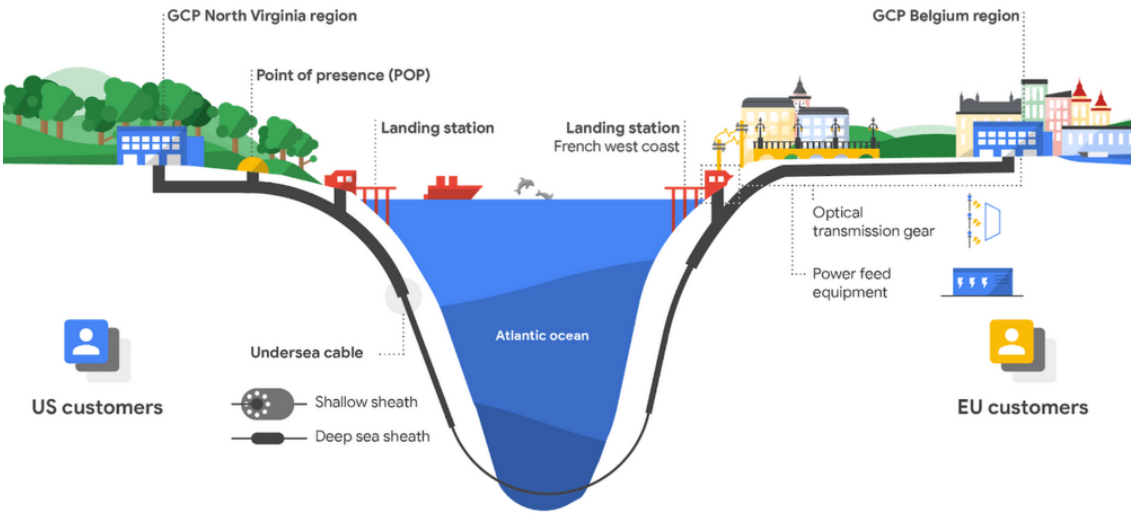


Figura 7: G. Porro, Google collega con un super cavo in fibra Europa e Stati Uniti, Wired, 5 febbraio 2021.

[41] S. E. Makris, N. Lordi and M. G. Linnell, "Metrics for measuring the robustness of the undersea cable infrastructure: A road to standardization," 2011 Second Worldwide Cybersecurity Summit (WCS), 2011, pp. 1-5.
[42] CSRIC WG4A—Final Report on Cable Landings, p. 4.

1.3 BREVE STORIA DEI CAVI SOTTOMARINI

Negli ultimi decenni, l'evoluzione delle telecomunicazioni ha segnato una rivoluzione senza precedenti nel modo in cui il mondo è connesso. Al cuore di questa trasformazione si trovano i cavi sottomarini per le telecomunicazioni, reti di fibre ottiche che si estendono per migliaia di chilometri sotto gli oceani del globo. Questi incredibili fili sottili sono diventati la spina dorsale del sistema di comunicazione globale, consentendo lo scambio di dati, voce e informazioni a velocità impensabili solo qualche tempo fa. Tuttavia, per comprendere appieno il ruolo cruciale che svolgono i cavi sottomarini nel panorama delle telecomunicazioni odierno, è essenziale esplorare la loro affascinante storia, caratterizzata da innovazioni tecnologiche, sfide tecniche e geopolitiche ed impatti socio-economici di vasta portata. In questo contesto, il presente paragrafo si propone di tracciare un viaggio nel tempo attraverso la storia dei cavi sottomarini e degli uomini che hanno reso possibile tutto ciò gettando luce sulle implicazioni che ha avuto sulle comunicazioni e sulla società nel corso degli anni.

La storia dei cavi sottomarini è suddividibile in diverse fasi che coincidono con altrettante scoperte tecnologiche. Nell'era del telegrafo, i conduttori di rame potevano trasportare solo il testo, di solito brevi telegrammi. Nell'era del telefono, la tecnologia dei cavi coassiali si era sviluppata a sufficienza per trasportare fino a 5.680 chiamate telefoniche simultanee[43]. E nell'odierna era della fibra ottica, fibre di vetro trasportano lunghezze d'onda multiple di luce laser, fornendo terabit di dati per telefonate, testi, pagine internet, musica e altro.

1.3.1 Era del Telegrafo

Il settore dei cavi sottomarini è stato per molto tempo monopolizzato dall'impero britannico. Basti pensare che per la fine del 1950 il 90% dei cavi veniva prodotto da aziende inglesi e per l'82%[44] (385,000 miglia nautiche di cavi marittimi) da una sola società: la *Telegraph Construction & Maintenance Company* (Telcon), nota oggi come Alcatel-lucent Submarine Networks. Il Regno Unito era la principale potenza navale e coloniale e necessitava del predominio delle comunicazioni su lunga distanza sia per ragioni di carattere logistico che militare. Il nostro percorso ha inizio proprio in Inghilterra, nel 19° secolo.

Come accennato nei paragrafi precedenti, i cavi sottomarini nascono come estensione dei telegrafi Morse; ne condividono tutt'oggi la stessa logica di funzionamento. Le prime costruzioni di telegrafi di Morse risalgono al 1840. William Cooke e Charles Wheatstone ottennero il primo brevetto per un

[43] S. Ash, The Story of Subsea Telecommunications & its Association with Enderby House, accessed at https://atlantic-cable.com/CableCos/EnderbysWharf/index.htm.
[44] Lawford G.L, Nicholsono l.r. *The Telcon Story, 1850-1950.* Telegraph Construction & Maintenance, 1950.

telegrafo elettronico nel 1839 e lo commercializzarono nel 1843. Bisognava solo capire come immergere questi cavi in acqua. Ciò fu reso possibile dall'intuizione di Faraday di utilizzare la gutta perca come isolante per i cavi sottomarini[45].

Il primo cavo sottomarino fu posto tra Calais e Dover dal piroscafo "Goliath" e venne finanziato da James and John Brett[46] ma durò pochi giorni. Difatti non erano state previste protezioni esterne ma solo dei pesi posti ogni sedicesimo di miglio. Un anno dopo fu sostituito da un nuovo cavo il cui design, basato su un brevetto di Robert S. Newall[47], era più robusto: comprendeva quattro conduttori di rame, ciascuno doppiamente rivestito con gutta perca, legato con canapa e pesantemente corazzato con fili di ferro. Questa versione migliorata ha esteso la vita utile dei cavi a un decennio. Dopo l'installazione, che avvenne il 13 Novembre 1851, John Brett inviò un messaggio speciale al futuro imperatore di Francia, Napoleone III, un atto che segnò simbolicamente il giorno in cui le telecomunicazioni sottomarine divennero un'industria. Il cavo segnò una rivoluzione sostanziale in molti settori. Basti pensare che per la prima volta, i prezzi delle azioni della Borsa di Parigi potevano essere visualizzati nella Borsa di Londra lo stesso giorno. Nel 1852 erano già diversi i cavi esistenti. Tuttavia, il rame utilizzato per i conduttori tendeva ad essere duro, fragile e scarsamente conduttivo, mentre l'isolamento della guttaperca era a volte grumoso e solo moderatamente flessibile.

Dopo i primi cavi degli anni 50 del 800 la sfida principale divenne la costruzione di un cavo Transatlantico. Il primo ad avere l'impulso per questa avventura fu un eccentrico imprenditore americano, Cyrus West Field. Così nel 1854 fondò la *New York, Newfoundland and London Telegraph Company* negli Usa. Tuttavia, l'impresa non avrebbe avuto possibilità di successo senza le finanze ed il know-how delle aziende inglesi. Per questo motivo Field si recò a Londra dove conobbe Brett ed insieme al quale diede luce alla *Atlantic Telegraph Company*. Quest'ultima nasce nel 1856 ed è la prima azienda a costruire un cavo Transatlantico tra Irlanda e Terranova nel 1858. Tuttavia, il cavo si ruppe dopo 334 miglia nautiche. Dopo questo evento ci furono altri due tentativi: nel giugno 1858 ricominciò l'operazione di posa ad opera delle navi USS Agamennone e USS Niagara che si incontrarono nel mezzo dell'Oceano e unirono le estremità dei loro cavi ma il progetto ebbe vita breve. Solo 400 furono i messaggi inviati. L'episodio sollevò numerose proteste da entrambe le parti

[45] La guttaperca è un materiale naturale che viene estratto dalla linfa di alcune specie di alberi. Si tratta di una resina gommosa e termoplastica. Quando veniva riscaldata, la guttaperca diventava malleabile e facilmente modellabile. Questa caratteristica la rendeva ideale per avvolgere i cavi sottomarini, fornendo un'efficace protezione contro l'acqua e l'umidità.
[46] Carter, L., Burnett, D. Drew, S. «Submarine Cables and the Oceans – Connecting the World.», *UNEP-WCMC Biodiversity Series No. 31* (ICPC/UNEP/UNEP-WCMC), 2009: 11-14
[47] R.S Newall, Facts and Observations Relating to the Invention of the Submarine Cable and to the Manufacture and Laying of the First Cable Between Dover and Calais in 1851, E. & F. N. SPON, London, 1882.

dell'Atlantico tanto che il Boston Courier sostenne che l'intero progetto fosse una frode finanziaria[48]. Per tranquillizzare gli investitori e l'opinione pubblica il governo britannico e la *Atlantic Telegraph Company* istituirono un comitato congiunto per indagare sulle ragioni dei fallimenti. Il rapporto che venne pubblicato nell'aprile 1861[49], giunse alla conclusione che la telegrafia oceanica fosse un ambito ancora tutto da scoprire ed elaborò alcune proposte: la più importante riguardava l'esigenza di standardizzare la misurazione della corrente elettrica e della resistenza (ciò portò al set di standard per l'Ampere, l'Ohm e Volt). Un nuovo e migliorato cavo fu posato con successo nel 1866 dalla Great Eastern Cable Ship[50]. Il nuovo e più resistente cavo forniva comunicazioni ragionevolmente affidabili a circa 12 parole al minuto attraverso l'Atlantico. Verso la fine del secolo i materiali tecnici utilizzati erano notevolmente migliorati sia per quanto concerne la protezione dei cavi che soprattutto per la loro capacità di segnalazione. Il personale impiegato per inviare e ricevere messaggi telegrafici nelle stazioni di trasmissione è stato gradualmente sostituito da segnalatori elettromeccanici. Le velocità di trasmissione aumentarono progressivamente e alla fine degli anni 1920 le velocità superiori a 200 parole al minuto divennero la norma.

La Telcon divenne velocemente l'azienda leader nel settore dei cavi sottomarini. La *The Eastern and Associated Telegraph Companies*[51] e *l'Anglo-American Telegraph Company* possedevano un monopolio virtuale sulle comunicazioni in tutto il mondo tanto che tutti i concorrenti erano stati costretti ad abbandonare il mercato. L'unico altro produttore rimasto era la *Siemens Brothers* che era diventato il più grande il più grande concorrente di *Telcon*. Sul finire di quest'epoca la sfida per i cavi sottomarini passò alla costruzione di cavi nel Pacifico che consentissero di collegare le colonie inglesi. Ciò venne commissionato alla Telcon e si realizzò nell'ottobre 1902 grazie ad un cavo che collegava l'Australia e la Nuova Zelanda passando per le isole Figi e l'isola di Fanning. Questi successi segnarono l'apice dell'epoca del telegrafo e convinsero il governo britannico a nazionalizzare diverse aziende. Nonostante la tecnologia alla base delle comunicazioni telefoniche fosse già stata positivamente sperimentata da Meucci e da Bell negli anni 70 del secolo precedente, il telegrafo rimaneva la soluzione più efficiente per le comunicazioni su grandi distanze.

---

[48] Carter, L., Burnett, D. Drew, S. «Submarine Cables and the Oceans – Connecting the World.» *UNEP-WCMC Biodiversity Series No. 31.*

[49] C. Wheatstone et al. "*Report of the Joint Committee Appointed by the Lords of the of the Committee of Privy Council for trade and the Atlantic Telegraph Compani to Inquire into the Construction of Submarine Telegraph Cables together with the Minutes of Evidence"* (Board of Trade and the Atlantic Telegraph Company), 1861, pp. 1.

[50] J.S Gordon, "A Thread across the Ocean: The Heroic Story of the Transatlantic Cable", Simon & Schuster, 2002.

[51] B.Glover, The Evolution of Cable & Wireless, Part 3, accessed at History of the Atlantic Cable & Submarine Telegraphy - Cable & Wireless (atlantic-cable.com).

Il telegrafo senza fili ottenne maggiore attenzione a partire della Prima guerra mondiale come mezzo di comunicazione tra Londra e le navi della Royal Navy nel Mediterraneo. La commercializzazione del telegrafo radio divenne un valido concorrente commerciale dei cavi. Difatti bisogna sottolineare come questo mezzo risultava essere più veloce dei cavi telegrafici (fino a tre volte) utilizzando un quinto della potenza e ad un ventesimo del costo. Le aziende telegrafiche subirono una forte battuta d'arresto a causa della concorrenza dei radio telegrafi e della grande depressione tanto che nel 1930 erano sopravvissute soltanto la Telcon e la Siemens. Queste si fusero nel 1935 per formare la *Submarine Cables*.

1.3.2 Era telefonica

Il primo cavo telefonico sottomarino venne posato nel 1891 dal General Post Office britannico nel canale della Manica. Tuttavia, a causa degli effetti distorsivi le comunicazioni potevano avvenire solamente a brevi distanze. Per superare tali problematiche furono necessarie due scoperte scientifiche: il brevetto del "cavo coassiale" nel 1880 ma che non venne utilizzato fino al 1921 e la scoperta del Polietilene che fu un passaggio chiave nella storia dei cavi[52]. Prima dell'introduzione del polietilene, la guttaperca veniva ampiamente utilizzata come isolante nei cavi sottomarini. Tuttavia, la guttaperca presentava alcuni svantaggi, tra cui la sua suscettibilità all'umidità e la tendenza a invecchiare e deteriorarsi nel tempo. È interessante notare come la guttaperca si trovasse per la maggior parte su alberi situati nelle colonie inglesi[53]. Questo fu uno dei motivi del monopolio inglese nella produzione di cavi. Inoltre, il polietilene è anche più economico e più facile da lavorare rispetto alla guttaperca. La sua produzione su larga scala è possibile, consentendo una maggiore disponibilità di cavi sottomarini a costi accessibili. La scoperta del Polietilene nel 1933 rese possibile chiamate transoceaniche e nel 1938 venne sviluppato un cavo coassiale da 1,7 pollici[54] rivestito in polietilene a più canali vocali [55] .

Pertanto, il polietilene consentiva comunicazioni chiare a medie distanze ma per le chiamate transoceaniche il discorso era diverso. Difatti era essenziale amplificare il segnale e per farlo era necessario inserire degli amplificatori all'interno dei cavi sottomarini. L'idea era stata sviluppata già nel 1865 ma non vi era la tecnologia necessaria per sviluppare il progetto. I problemi tecnici erano diversi: racchiudere l'amplificatore in un involucro a tenuta stagna ma ottenere comunque l'accesso

[52] Il polietilene è un materiale termoplastico con eccellenti proprietà isolanti elettriche, resistenza all'umidità e resistenza chimica. Queste caratteristiche consentono ai cavi sottomarini protetti in polietilene di offrire una maggiore durata, prestazioni migliori e una maggiore affidabilità rispetto ai cavi in guttaperca.
[53] N. Starosielski, "The Undersea Network", Duke University Press, 2015.
[54] Le dimensioni di un cavo coassiale sono definite dal diametro del dielettrico tra il conduttore interno e quello esterno.
[55] Carter, L., Burnett, D. Drew, S. «Submarine Cables and the Oceans – Connecting the World.», *UNEP-WCMC Biodiversity Series No. 31* (ICPC/UNEP/UNEP-WCMC), 2009: 11-14

al percorso di trasmissione, integrare l'amplificatore nel cavo, fornirgli l'alimentazione necessaria e dissipare il calore che avrebbe prodotto. Ancora più importante, tutti gli amplificatori dovevano essere affidabili in modo da non dover essere recuperati e sostituiti. Il primo amplificatore venne aggiunto al cavo coassiale da Anglesey a Port Erin posato nel 1943[56]. Il primo cavo telefonico transatlantico dotato di ripetitori venne costruito dall'azienda americana Simplex e segnò l'inizio del coinvolgimento degli Stati Uniti nella produzione di cavi sottomarini. Nel 1955-56 vennero posati i primi due cavi telefonici transoceanici tra la Scozia e Terranova. Il cavo venne denominato TAT-1 ed effettuò 707 chiamate nel suo primo giorno operativo. Esso poteva ospitare fino a 36 chiamate simultaneamente ad un costo di 1$ per minuto.

Ad ogni scoperta conseguiva una nuova sfida. Infatti, i ripetitori erano costosi e il miglioramento della qualità delle comunicazioni cresceva con il numero di ripetitori installati sul singolo cavo. Questo rendeva sostenibili economicamente solo le rotte ad alta densità di comunicazione. L'ultimo dei cavi a bassa larghezza di banda fu il TAT-7. Per tali ragioni, diverse comunicazioni transoceaniche si appoggiavano sul sistema satellitare. Durante gli anni 70 e primi anni 80 i satelliti divennero gradualmente la modalità predominante di trasmissione per la telefonia internazionale. Tuttavia i satelliti non garantivano comunicazioni sicure come quelle dei cavi sottomarini e non potevano trasmettere con la stessa qualità di segnale. Nel 1986 si conclude l'era della telefonia con la posa dell'ultimo sistema STC 14 MHz tra l'India e gli Emirati Arabi Uniti[57].

1.3.3 Era della fibra ottica

Fino agli anni 80 le comunicazioni passavano tramite i satelliti o i cavi telefonici sottomarini. Tuttavia la fibra ottica era oggetto di ricerche e sperimentazioni già dagli anni 60. Nel 1962 venne realizzata la prima emissione di luce coerente da parte di un laser a semiconduttore da gruppi di ricerca della General Electric e dell'IBM, negli Stati Uniti. L'origine della fibra ottica risale a pochi anni più tardi. Nel 1966, due giovani ricercatori dell'STL, Charles Kuen Kao e il suo collega George Alfred Hockham, svilupparono l'idea che le che le informazioni potessero essere trasportate non come onde radio o da correnti elettriche, ma da fasci di luce laser, trasportati da sottili fibre di vetro.

"Una fibra di materiale vetroso costruita in una struttura rivestita con un con un diametro del nucleo di circa λ° e un diametro complessivo di circa 100 λ° rappresenta una guida d'onda ottica pratica con un importante potenziale come nuova forma di mezzo di comunicazione (...) rispetto ai cavi coassiali

[56] Scenk, I. Waldick, "1990 World's Submarine Telephone Cable Systems", U.S. Department of Commerce, National Telecommunications and Information Administration, 1990, at pp.87
[57] D.R Bournett, R. B et al. (2013). *Submarine Cables: The Handbook of Law and Policy.* Martinus Nijhoff

e ai sistemi radio esistenti, questa forma di guida ha un'ampia capacità di trasporto delle informazioni e possibili vantaggi nel costo del materiale di base." [58]

A differenza delle epoche precedenti, fin dall'inizio i produttori si erano prefissati di sviluppare sistemi in grado di attraversare oceani più profondi, per cui i cavi e i ripetitori erano già pronti per il passo successivo: un sistema che attraversasse l'Oceano Atlantico. Il primo cavo internazionale arrivò nel 1986 e collegò Uk e Belgio mentre nel 1988 venne costruito il primo cavo transatlantico che collegava USA, Uk e Francia. Questo era il cavo TAT-8 e segnò il superamento dei satelliti per le comunicazioni in termini di velocità, volume di dati e costi.

1.3.4. Sviluppi tecnologici

Per trasmettere informazioni in entrambe le direzioni utilizzando fibre ottiche, erano necessarie due fibre separate. Tuttavia, un singolo cavo può contenere più di due fibre. L'obiettivo era separare i percorsi di trasmissione in cavi diversi. Per facilitare questo processo venne sviluppato un contenitore sommerso chiamato "branching unit" (BU). La BU permette di separare i percorsi delle fibre e include circuiti di commutazione per gestire l'alimentazione del sistema[59]. In altre parole, la BU permetteva (e lo permette tutt'oggi) di organizzare le fibre ottiche in modo che possano trasmettere le informazioni in direzioni diverse (anche verso altre Cable Landing Station) all'interno di un sistema di comunicazione. Il TaT-8 venne sviluppato da tre fornitori diversi. Nel 1986 la velocità e qualità del segnale trasmesso dai cavi in fibra migliorò ulteriormente grazie all'invenzione dell'EDFA ("Erbium-Doped Fiber Amplifier") da parte del Professor Payne. L' EDFA è un dispositivo utilizzato nella tecnologia delle comunicazioni ottiche per amplificare segnali luminosi trasmessi attraverso una fibra ottica[60]. L'altra specialità dell'EDFA era la sua capacità di poter amplificare simultaneamente segnali a due o più lunghezze d'onda. Questo consentiva di utilizzare fino a 16 lunghezze d'onda per coppia di fibre[61]. La spaziatura tra le lunghezze d'onda consentì anche di utilizzare tecnologie come il Wavelength Division Multiplexing (WDM[62]), che suddivide lo spettro ottico in diverse bande di

[58] S. Ash, The Story of Subsea Telecommunications & its Association with Enderby House, accessed at https://atlantic-cable.com/CableCos/EnderbysWharf/index.htm.
[59] Wei Jiang, Submarine Optical Cable Engineering, Academic Press, 2018, pp. 9-10
[60] L'EDFA utilizza una fibra ottica droppata con impurità di erbio, che è un elemento chimico. Quando un segnale ottico passa attraverso questa fibra droppata con erbio, l'impurità di erbio assorbe la luce e la emette in modo coerente, amplificando così il segnale luminoso. In sostanza, l'EDFA amplifica i segnali ottici senza dover convertire il segnale in forma elettrica, migliorando così la velocità e l'efficienza della trasmissione ottica nelle reti di comunicazione.
[61] La spaziatura tra le lunghezze d'onda si riferisce alla differenza di frequenza o lunghezza d'onda tra i segnali ottici trasmessi attraverso una fibra ottica
[62] Più segnali ottici di diverse lunghezze d'onda (colori) vengono trasmessi insieme attraverso un singolo cavo in fibra ottica e separati nuovamente per un ulteriore instradamento aumentando così la capacità di trasmissione di dati del cavo. Vedi Charles A. Brackett, "Dense Wavelength Division Multiplexing Networks: Principles and Applications," IEEE Journal on Selected areas in Communications, vol. 8, no. 6 (August 1900), pp. 948-964;

frequenza o lunghezze d'onda, ognuna delle quali può trasportare un segnale indipendente. Questo aumentò notevolmente la capacità di trasmissione dei cavi sottomarini in fibra ottica e consentì di gestire un maggior volume di dati attraverso la stessa infrastruttura.

In questo periodo, la quantità di dati trasmessi sui sistemi sottomarini cominciò a superare il traffico vocale. La fibre di vetro disponevano di una capacità di 12.000 canali rispetto ai 5.500 dei vecchi TAT e soprattutto la qualità era nettamente migliore[63]. I presupposti per la crescita esponenziale dei cavi sottomarini e della loro importanza furono da una parte le scoperte tecnologiche citate e dall'altra il contesto economico e sociale. Infatti gli anni 90 sono ricordati come il decennio della globalizzazione, delle liberalizzazioni, della nascita di Internet su larga scala e del mercato comune europeo. La capacità della lunghezza d'onda è aumentata rapidamente dall'inizio degli anni Duemila, con capacità di 10 Gbps che sono entrate per la prima volta nel mercato intorno al 2003, e le lunghezze d'onda di 100 Gbps, apparse nel 2010[64]. Parallelamente all'aumento della capacità del canale, è stato sviluppato il concetto di "upgrade del sistema". Dalla prima metà degli anni Duemila, è diventato possibile per i proprietari dei cavi sottomarini intervenire sulle componenti relative alla sezione terminale della linea sottomarina (SLTE) per aumentare la capacità, senza dover costruire un sistema di cavi completamente nuovo. Da allora, gli aggiornamenti dei sistemi sono diventati il modo più economico per aggiungere capacità lungo un percorso di cavi sottomarini, con la possibilità di attivazione in un lasso di tempo molto più breve rispetto alla implementazione di nuovi cavi. I progressi nelle tecnologie dei cavi sottomarini in fibra ottica, per la trasmissione, la ricezione e l'amplificazione dei segnali ottici, hanno portato la capacità di carico media per i segnali di telecomunicazione sottomarini ad aumentare da 25 a 60 terabit al secondo (Tbps) tra il 2014 e il 2019. I recenti sviluppi tecnici hanno consentito ai cavi di telecomunicazione sottomarini di raggiungere capacità di carico fino a 250 Tbps. Il cavo sottomarino MAREA che opera tra Virginia Beach, VA, e Bilbao, Spagna, può trasmettere fino a 200 Tbps. Quando è stato completato nel 2017, i suoi proprietari – Microsoft, Facebook e Telxius (una sussidiaria della società di telecomunicazioni spagnola, Telefónica) – hanno dichiarato che si trattasse del "cavo sottomarino con la più alta capacità che avesse mai attraversato l'Atlantico"; con otto coppie di fibre e una capacità di progetto iniziale stimata di 160 Tbps" opera "oltre 16 milioni di volte più velocemente della connessione media di Internet domestico"[65]. MAREA ha utilizzato un design aperto, che consente l'integrazione di nuove

[63] D.R Bournett et al. *Submarine Cables: The Handbook of Law and Policy, Op.Cit*
[64] V. Francola, A.Gordon, Mensah, "L'industria dei cavi sottomarini: qualche elemento introduttivo", Astrid Rassegna (Laboratorio sull'Ecosistema Digitale Astrid, 2021)
[65] Suresh Kumar, "Celebrating the Completion of the Most Advanced Subsea Cable Across the Atlantic," Official Microsoft Blog, September 21, 2017, https://blogs.microsoft.com/blog/2017/09/21/celebrating-completion-advancedsubsea-cable-across-atlantic/.

apparecchiature di rete più performanti. Nel 2018, i proprietari di MAREA hanno annunciato di aver integrato nuove tecnologie nel sistema, aumentandone la capacità da 160 Tbps a 200 Tbps.

1.4 PROFILI DI CARATTERE TECNICO E FUNZIONALE

1.4.1 Come vengono posati i cavi sottomarini

Come si sarà intuito, siamo di fronte ad un'infrastruttura estremamente capillare e interconnessa. L'elemento marittimo sottopone i cavi a importanti stress fisici. La maggior parte dei rischi trova la sua causa nell'ambiente subacqueo con i suoi fenomeni imprevedibili e travolgenti. Il paradosso del cavo sottomarino è che deve risultare tanto resistente quanto flessibile e di piccole dimensioni. Tuttavia, nessun materiale consentirà mai di costruire dei cavi in grado di resistere a qualsiasi condizione. Per questo motivo, il modo in cui i cavi vengono installati gioca un ruolo fondamentale.

La prima operazione che deve essere svolta è quella di selezione della rotta che verrà percorsa dal cavo sottomarino. Questa operazione presuppone innanzitutto uno studio di fattibilità il cui scopo è quello di valutare i rischi e i pericoli a cui il sistema di cavi può essere esposto durante la sua vita utile. Così facendo l'azienda è in grado di capire i costi a cui sarà sottoposto il cavo e le richieste di permesso che successivamente si dovranno ottenere dai singoli stati per poter costruire il sistema. Quest'ultima analisi è fondamentale per capire quali sono le zone da evitare per via di rischi di natura geopolitica o di contese territoriali in atto. Lo studio di fattibilità tecnica è invece chiamato "Studio Desktop". È generalmente condotto da geologi marini con esperienza di ingegneria dei cavi che raccolgono tutte le informazioni idrografiche e geologiche disponibili sulla regione pertinente. In questa fase è di cruciale importanza mappare i fondali marini. Ciò può essere fatto tramite la tecnica dell'"Eco sondaggio" o l'analisi "multibeam"[66].

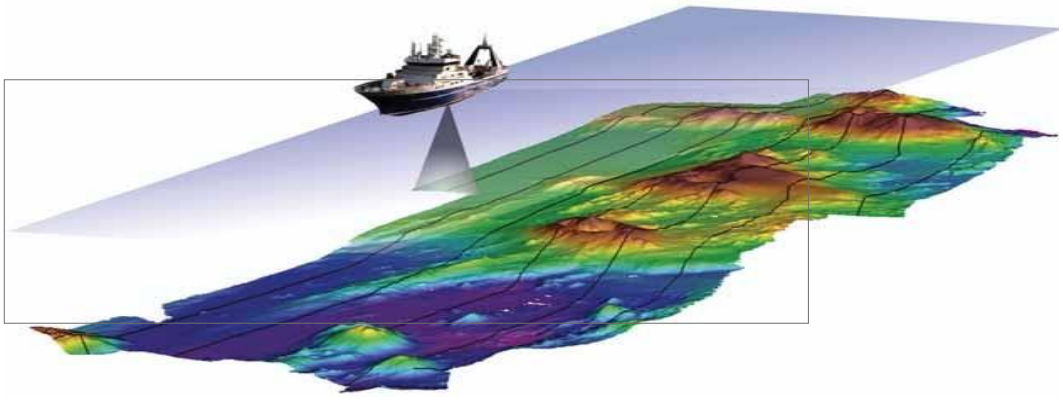


Figura 8: Una nave da rilevamento, dotata di un sistema di mappatura multibeam e guidata dalla navigazione satellitare, traccia il fondale marino per fornire una copertura totale con rilevamenti di profondità lungo una fascia di fondale che può essere larga 20 k

[66] E' una tecnica utilizzata per misurare la profondità dell'acqua in un determinato punto. Si basa sulla trasmissione di onde sonore nell'acqua e sulla misurazione del tempo impiegato per il loro riflesso dal fondale marino.

Le navi possono richiedere anche un mese per caricare il materiale necessario alla spedizione. La complessità di queste operazioni è causata dalla lunghezza dei cavi che devono essere avvolti in dei particolari serbatoi.

Quando un cavo entra in acqua è influenzato dalle condizioni marine e dalle condizioni della nave che lo deposita. I tre parametri chiave sono la velocità della nave sul terreno, la velocità a cui il cavo viene posato e la profondità dell'acqua. Come anticipato i cavi vengono posati in due modi: direttamente sul fondale marino oppure sepolti in modo che siano protetti maggiormente. Questa seconda opzione si predilige per i cavi che si estendono attraverso la piattaforma continentale fino ad una profondità di 1000-1500 m[67]. Queste profondità si hanno quando il cavo viene attaccato direttamente ai tombini della spiaggia. Per questi attacchi diretti vengono utilizzati dei sommozzatori che manualmente uniscono il cavo al punto di uscita della spiaggia. Questo punto di uscita è l'ultima zona terrestre dei cavi. Per la sepoltura viene utilizzato un aratro marino. Viceversa, se si opera a profondità superiori ai 1000-1500 metri, il cavo verrà posato sul fondale marino senza alcuna sepoltura. Questa profondità corrisponde all'attuale capacità dei moderni pescherecci a strascico.

E' altrettanto importante ricordare che l'operazione di posa non consiste solo nel far calare il cavo sul fondale per tutta la sua lunghezza. Si pensi alla posa dei ripetitori, di norma ogni 60-90km, che richiedono di fermarsi e posarli con grande cura. Allo stesso modo è possibile unire estremità

Figura 9: Figura 9: Fonte: Op. Cit, Submarine cables: handbook of law and policy, 2013.

[67] Carter, L., Burnett, D. Drew, S. «Submarine Cables and the Oceans – Connecting the World.», *UNEP-WCMC Biodiversity Series No. 31* (ICPC/UNEP/UNEP-WCMC), 2009: pp. 23-24

dei cavi (in seguito a danneggiamenti) ma si tratta di procedure molto costose e specializzate. Parte di questi costi sono legati ai numerosi permessi necessari per operare nelle ZEE dei diversi paesi per cui passa il cavo. E' il caso dell'India che richiede fino a 7 diversi permessi oltre all'obbligo di avere almeno 1/3 dell'equipaggio di nazionalità indiana sulla nave[68].

1.3.2 Come vengono riparati i cavi

La riparazione dei cavi sottomarini per le telecomunicazioni è un obbligo in capo alle aziende proprietarie o che hanno costruito il cavo ed è un processo complesso che richiede competenze tecniche specializzate. Si tratta di un tema particolarmente rilevante non solo dal punto di vista tecnico ma anche politico. Gli stati dipendono dai cavi ma non li posseggono e questo riduce il loro margine di manovra in caso di un danno all'infrastruttura. Inoltre, i privati sono meno incentivati alla manutenzione e protezione dei cavi di quanto potrebbero esserlo gli stessi governi visto che essi devono realizzare un profitto. Per poter comprendere l'impatto che può avere il danneggiamento di un cavo è necessario conoscere quali sono i tempi e le difficoltà nel riparare questi cavi.

Come già descritto, le aziende dedicano molta attenzione e tempo nella prevenzione e sicurezza dei cavi tramite appositi studi che limitino i rischi di danneggiamento dei cavi ma ciò non è sempre possibile. Sono molte le variabili (umane e naturali) che influiscono sul buon funzionamento del sistema. Oltre ai costi diretti legati alla riparazione stessa, è importante considerare anche i costi indiretti associati all'interruzione dei servizi di comunicazione e ai ritardi nella ripresa delle operazioni. Ne consegue che alle aziende si richiede di intervenire nel momento stesso in cui si rileva il danneggiamento. Per questo motivo si è elaborato il cd *Contratto di Manutenzione*[69]. Si tratta di un accordo in base al quale i mari vengono divisi in diverse aree all'interno delle quali si posizionano un determinato numero di navi specializzate in riparazioni e di depositi di stoccaggio dei pezzi di ricambio dei cavi. Questi asset non appartengono ad una sola azienda ma sono finanziati, e quindi utilizzabili, da un consorzio di aziende proprietarie di cavi in quella determinata regione. Il funzionamento è simile a quello delle aree riservate ai soci di determinate aziende negli aeroporti di tutto il mondo. Questo rende sostenibile

[68] Ciò è attribuibile in primo luogo, alla paura dell'India del terrorismo nelle zone marittime dell'India (ad esempio, gli attacchi terroristici del 2008 a Mumbai hanno avuto origine dal mare) e in secondo luogo, i terroristi in quell'attacco hanno usato telefoni cellulari e VoIP. **Specificata fonte non valida.**
Vedi K. Bressie and M. Findley, "Coping with India's New Telecom: Equipment Security Requirements and Indigenous Innovation" (March 2102) 62 Submarine Telecoms Forum 15–19 at 16 available online at http://www.subtelforum.com/articles/wp-content/STF-62.pdf and R. Rapp et al., "India's Critical Role in the Resilience of the Global Under- sea Communications Cable Infrastructure" (May–June 2012) 36(3) Strategic Analysis, 375–383 at 378–379.)

[69] Per approfondire vd. M. Sechrist, Cyberspace in Deep Water: Protecting Undersea Communication Cables By Creating an International Public-Private Partnership, Harvard Kennedy School, 2013.

economicamente il possesso di navi specializzate pronte a salpare in qualsiasi momento dell'anno e in ogni regione. Queste aziende pagano una quota fissa all'anno per i costi fissi delle strutture oltre ad una quota aggiuntiva quando si decide di utilizzare il servizio per i costi variabili (benzina, personale ecc.). Pertanto, quando si costruiscono i cavi sottomarini non si calcola esclusivamente la distanza necessaria a collegare le due estremità ma un kilometraggio nettamente maggiore che renda sempre disponibile nei magazzini la fibra ottica necessaria ad intervenire.

Sul cavo sono posizionate delle apparecchiature che rilevano la perdita di luce o di segnale e lo comunicano ai punti di approdo posizionati alle due estremità del cavo. In automatico il sistema reindirizza il segnale su altri cavi. Difatti ogni cavo possiede una sezione delle proprie fibre che viene tenuta nascosta o inutilizzata in modo da poter essere sfruttata in casi di guasti di altri cavi[70]. Nel giro di un minuto viene contattato un tecnico del *Centro operativo di rete* che analizzerà manualmente la situazione per capire se è possibile risolverla da remoto. Nel giro di alcune ore viene inviato il tecnico direttamente al punto di instradamento della fibra dove utilizzerà il *Riflettometro ottico a dominio del tempo* per determinare l'esatto punto di danneggiamento della fibra[71]. Una volta individuato il punto, il cavo viene tagliato completamente e le estremità vengono portate in superficie con un piccolo sommergibile o con lunghi ganci. A meno che i mari non siano agitati, questa operazione di doppia giunzione può richiedere circa 20 ore dall'inizio alla fine.

Una delle estremità viene portata a bordo della nave mentre l'altra viene attaccata a una boa e fatta galleggiare sulla superficie dell'oceano. La parte di cavo posizionata sulla nave viene giunta con il nuovo cavo sottomarino e si verifica che il collegamento funzioni. Se non ci sono problemi la nave si riavvicina alla boa e unisce il cavo che vi è attaccato con quello fatto riparare a bordo della nave. Questo tipo di operazione può richiedere tra i 3 ed i 5 giorni in condizioni normali ed un costo diretto di almeno 3 milioni[72]. A questi costi vanno aggiunti tutti quelli indiretti sostenuti dagli stati e dai singoli cittadini per l'impossibilità di usufruire del servizio.

[70] Ivi, pp.100.
[71] Viene inviato un segnale di luce e calcolando quanto tempo ci mette a tornare indietro si è in grado di stabilire il punto di rottura della fibra.
[72] W. Rain, Problems faced by Industry in the repair of damaged submarine telecommunications cables inside maritime jurisdictional claims, National University of Singapore, 2009.

1.5 I SETTORI COINVOLTI

Ora che abbiamo delineato il funzionamento tecnico dei cavi e la loro infrastruttura possiamo analizzare quale sia la loro influenza in diversi settori della nostra vita. Questo primo passaggio ci aiuterà a comprendere le dimensioni del settore e perché sia così rilevante.

A causa della velocità con cui le informazioni potevano essere scambiate, l'uso di cavi sottomarini si è rivelato un catalizzatore per la globalizzazione e l'impegno internazionale in quanto essi hanno ridotto significativamente i tempi di comunicazione tra i continenti. I cavi sottomarini sono diventati rapidamente importanti risorse internazionali per le agenzie di stampa, le compagnie commerciali e di navigazione, i governi e le loro forze armate e il pubblico. Hanno dapprima consentito ai capitani delle navi e alle compagnie di comunicare da porti lontani, migliorando immediatamente la gestione logistica e hanno notevolmente migliorato la comunicazione tra vari stati e colonie aiutando le relazioni diplomatiche in tempo di pace e facilitando la comunicazione durante i conflitti. Storicamente la domanda di cavi sottomarini era proporzionale alle forze navali di una nazione, al numero di colonie e la minaccia percepita di conflitto. Il governo britannico, ad esempio, considerava i cavi di importanza strategica in particolare per le questioni coloniali a lunga distanza e questo fu il motivo del suo importante contributo all'industria internazionale della posa dei cavi[73]. Oggigiorno le cose sono cambiate. Tutti i paesi necessitano di forti collegamenti sottomarini senza i quali non potrebbero esercitare la maggior parte dei compiti primari di uno stato come la difesa e la crescita economica[74].

Come già anticipato i cavi rappresentano l'infrastruttura tramite cui passa il 99% delle nostre comunicazioni e operazioni tramite internet. Questo è dovuto principalmente ai minori costi ma soprattutto alla maggiore velocità di cui dispongono se confrontati con i satelliti. Basti pensare che i satelliti sono più lenti di almeno 400 millisecondi rispetti ai cavi[75]. Si tratta di una differenza gigantesca quando parliamo del passaggio di dati. Per moltissimi settori anche solo un millisecondo può essere cruciale.

1.5.1 Il rischio per il sistema finanziario

Secondo le stime della Federal Reserve statunitense, ogni giorno circa 10.000 miliardi di dollari (circa quattro volte il PIL annuale del Regno Unito) vengono trasmessi attraverso i cavi sottomarini. Inoltre, la Society for Worldwide Interbank Financial Telecommunication (SWIFT),

[73] K. Young, Semaphore: The Economic Importance of Submarine Cables, Sea Power Centre Australia, 2012.

[75] Vedi CISCO System, "Reliable Signaling System 7 (SS7) Transport Over Satellite Links," White Paper, 2005. **Specificata fonte non valida.**

che fornisce il quadro internazionale per circa 11.000 istituzioni finanziarie per condurre una media di 15 milioni di transazioni al giorno, dipende interamente dai cavi sottomarini[76]. Inoltre è stato stimato che, in seguito ad un danno a tutte le landing stations, l'impatto economico diretto per l'Australia sarebbe di 2,2 milioni di dollari al giorno mentre quello indiretto di 3,3 milioni[77]. Le conseguenze economiche variano fortemente da paese a paese in base al numero di cavi e di landing stations si cui è possibile reindirizzare il volume di dati trasmesso. Ad esempio, il Canada avrebbe un impatto prossimo allo zero per via del suo collegamento terrestre con gli Stati Uniti.

In un mondo così altamente interdipendente, le onde d'urto derivanti da una grave interruzione dei cavi in un importante centro finanziario come Londra, New York, Hong Kong o Singapore sono potenzialmente catastrofiche. Come afferma Karl Rauscher (presidente emerito dell'Institute of Electrical and Electronics Engineers e autore di un importante rapporto sui rischi associati ai cavi sottomarini[78]): "L'impatto di un tale guasto sulla sicurezza internazionale e sulla stabilità economica potrebbe essere devastante... Non è chiaro se la civiltà possa riprendersi dal fallimento di una tecnologia che è stata adottata così rapidamente senza un piano di riserva... Senza (la rete), il mercato economico-finanziario mondiale si bloccherebbe immediatamente". In parole povere, se un avversario riuscisse a portare a termine un attacco contro l'infrastruttura dei cavi sottomarini britannici, il risultato sarebbe un disastro finanziario di dimensioni senza precedenti. Secondo l'ex capo dello staff della Federal Reserve, Steve Malphrus: "Quando le reti di comunicazione vanno in tilt, il settore dei servizi finanziari non si ferma. Si arresta di colpo"[79].

Conseguenze analoghe si sono riscontrate in diversi casi. Uno dei più rilevanti risale al terremoto del 2008 nei pressi dello stretto di Luzon. Un terremoto di magnitudo almeno 6,7 ha innescato una frana sottomarina vicino alla giunzione delle placche tettoniche eurasiatica e filippina. Dall'inizio delle interruzioni, una corrente con una velocità media di circa 20 km/ora ha percorso oltre 330 km. Il guasto ha riguardato 9 degli 11 cavi operanti in quell'area e i danni si sono estesi fino ad una profondità di 4000 metri[80]. Sono state necessarie sette settimane e undici navi (pari al 40% della flotta globale) per riparare i danni causati ai cavi. La capacità di comunicazione tra Taiwan e USA è crollata del 40%. Il 98% delle comunicazioni di Taiwan con la Malesia,

[76] Rishi Sunak, Undersea Cables: Indispensable, Insicure, Policy Exchange, 2017.
[77] al., M. G. (2009). Submarine Cable Network Security. *APEC Submarine Cable Workshop Group, 2013.*
[78] Karl Frederick Rauscher, ROGUCCI - The Report, Proceedings of the Reliability of Global Undersea Cable Communications Infrastructure Study & Global Summit, IEEE Communications Society, 2010. **Specificata fonte non valida.**
[79] Commander Michael Matis , The Protection of Undersea Cables: A Global Security Threat, U.S. Army War College, 2012.
[80]R. Singel, Fiber Optic Cable Cuts Isolate Millions From Internet, Future Cuts Likely, Wired Magazine, January 2008, accessed at https://www.wired.com/2008/01/fiber-optic-cab/

Singapore, Thailandia e Hong Kong è stato interrotto[81]. L'accesso agli strumenti bancari, prenotazioni di aerei ed email è stato impossibile o fortemente rallentato. "Le contrattazioni del won coreano si sono per lo più fermate a causa del problema di comunicazione" secondo una banca coreana.[82] Il medesimo problema coinvolse tutte le agenzie di trading le cui transizioni risultarono fortemente rallentate. Appare chiaro come l'attuale sistema economico mondiale necessiti dei cavi sottomarini per poter esistere. Ciò è reso ancora più grave dalla mancanza di un piano di riserva. Come lo stesso K. Rauscher ha sottolineato, gli Stati Uniti possono reindirizzare sulle comunicazioni satellitari solo il 7% del proprio traffico digitale.

1.5.2 Impatto sul settore militare

L'interruzione di un cavo vicino l'Egitto nel 2008 ha causato rapidamente "una perdita del 60% della capacità commerciale e militare nella regione del Golfo[83]. Per il Generale Pollett, Direttore dell'Agenzia per i sistemi informativi della Difesa statunitense, si trattava di uno scenario da incubo. Gli Stati Uniti Stati Uniti avevano bisogno di una connessione veloce e ininterrotta per comunicare con il Medio Oriente. In un briefing del 20 febbraio 2009, il tenente colonnello Donald Fielden, comandante del 50° Squadrone Comunicazioni dell'Aeronautica Militare di Shriever, ha dichiarato che le rotture dei cavi hanno ridotto i voli degli UAV (*Unmanned aerial vehicle*[84]) che operano dalla base aerea di Balad, in Iraq, da "centinaia di sortite di combattimento al giorno" a " "decine di sortite al giorno"[85]. Questo episodio ha bloccato una delle basi americane più grandi presenti in Iraq e annullato la maggior parte delle operazioni statunitensi nella regione. Quando gli UAV "are the only game in town" l'affidabilità della rete globale è di primaria importanza[86]. Questo episodio sottolinea come interi settori possono essere bloccati anche solo da un rallentamento di internet. Non è necessario un totale blackout. Difatti gli UAV sono comandati da una base aerea situata a Las Vegas e perché ciò sia possibile è necessaria una latenza minima. Come nel caso delle transizioni finanziarie anche solo un millisecondo può fare la differenza ma in questo caso tra la vita e la morte. Nel 2010, gli UAV hanno volato per 190.000

---

[81] M. Sechrist, Cyberspace in Deep Water: Protecting Undersea Communication Cables By Creating an International Public-Private Partnership, Harvard Kennedy School, 2013.
[82] BBC News, Asia communications hit by quake, December 2006. Accessed at http://news.bbc.co.uk/2/hi/asia-pacific/6211451.stm
[83] Ivan Seidenberg, "Keynote Address: Customer Partnership Conference," Defense Information Systems Agency (DISA) Customer Partnership Conference, April 21, 2009.
[84] Si fa riferimento agli aeromobili senza pilota, comunemente noti come droni che vengono utilizzati dagli eserciti con compiti di sorveglianza aerea e supporto ravvicinato alle truppe in combattimento.
[85] Nick Lordi, "Air Force Cybersecurity Article Points," Telcordia Technologies, Inc., unpublished article.
[86] Noah Schactman, "CIA Chief: Drones 'Only Game in Town' for Stopping Al Qaeda," Wired Magazine, May 19, 2009. Accessed at http://www.wired.com/dangerroom/2009/05/cia-chiefdrones-only-game-in-town-for-stopping-al-qaeda/#ixzz0e8GDppPM

ore e l'Air Force stima che avrà bisogno di più di un milione di ore di volo UAV all'anno per essere pronta per le guerre future[87]. Anche il Dipartimento di Stato e le sue sedi diplomatiche e consolari dipendono fortemente dal traffico globale ininterrotto di cavi sottomarini.

Un ulteriore esempio della dipendenza del settore della Difesa dai cavi sottomarini è rappresentato dalla creazione del *Global Information Grid (*GiG) da parte del Dipartimento della Difesa statunitense[88]. Il GIG può essere descritto come una rete globale che può essere utilizzata per controllare uno spazio di battaglia globale[89]. Anche se si pensa che sia una rete privata sicura, si tratta principalmente di porzioni, o partizioni, del sistema di telecomunicazioni internazionale acquistate privatamente e disponibili a qualsiasi azienda o persona che possa pagare per accedervi. Se questa rete fosse compromessa vi sarebbero delle conseguenze catastrofiche per la sicurezza nazionale degli Stati Uniti. Tutte le comunicazioni militari sarebbero vulnerabili e anche il sistema logistico dell'esercito è basato sul sistema GIG. La guerra moderna ha portato ad una sempre maggiore interconnessione tra i vari sistemi d'arma, di comunicazione e di logistica con lo scopo di muovere in sincrono ogni attore sul campo e renderlo sempre informato. Tuttavia, questi sistemi hanno aumentato i rischi in quanto basta una piccola intromissione nel sistema per realizzare un effetto domino. Questi esempi si inseriscono nel nuovo concetto di Network Centric Warfare (NCW) che rappresenta la risposta con cui il comparto militare si adegua alla condotta delle operazioni nell'era dell'informazione e delle minacce ibride[90]. Una parte importante dei dati del Dipartimento della Difesa che viaggiano su cavi sottomarini è costituita da video di veicoli aerei senza pilota (UAV). Risulterebbe ancora più coinvolto dalla rottura di un cavo sottomarini il settore dell'intelligence. Difatti i servizi segreti necessitano di mezzi di sorveglianza che solo in una piccola misura si poggiano sulla tecnologia satellitare. Fondamentalmente una rottura dei cavi in fibra renderebbe l'intelligence "ceca".

---

[87] Commander M. Matis, The Protection of Undersea Cables: A Global Security Threat, U.S Army War College, Pennsylvania, 2012.

[88] Il GIG è "un sistema che racchiude l'insieme di capacità informative end-to-end, interconnesse a livello globale, per la raccolta, l'elaborazione, l'archiviazione, la diffusione e la gestione delle informazioni su richiesta dei soldati, dei responsabili politici e del personale di supporto." Definizione tratta dal sito web del *National Institute of Standards and Technology*, accessibile a https://csrc.nist.gov/glossary/term/global_information_grid

[89] Robert Fonow, Cybersecurity Demands Physical Security, SIGNAL MAG., Feb. 2006, at 43, 44, https://www.afcea.org/signal-media/cybersecurity-demands-physical-security

[90] Il termine identifica, in senso lato, una combinazione di elementi dottrinari, procedurali, tecnici, organizzativi e umani che, opportunamente collegati fra loro ("messi in rete" ovvero "networked", secondo la terminologia anglosassone), interagiscono creando una situazione di decisiva superiorità per la forza che ne dispone. Vedi "La trasformazione Net-Centrica e il futuro dell'interoperabilità multinazionale e interdisciplinare", Amm. G. di Paola, Capo di Stato Maggiore della Difesa, https://www.difesa.it/InformazioniDellaDifesa/periodico/IlPeriodico_AnniPrecedenti/Documents/La_Trasformazione_Net-Centrica.pdf

La rottura dei cavi può avere ripercussioni su altri settori. Secondo una simulazione del governo australiano, se uno o più cavi andassero offline, i responsabili del traffico aereo non sarebbero in grado di far atterrare gli aerei perché non potrebbero controllare chi vi è all'interno[91]. Medesimo discorso vale per l'ambito sanitario come dimostrato dal virus "Wannacry" del 2017 che ha messo in ginocchio gli ospedali britannici. Il malware, che si basava su una tecnologia creata dall'NSA per infettare i sistemi basati su Microsoft Windows, era in grado di criptare tutti i file presenti su quel computer e di diffondersi su tutti i dispositivi che si connettevano alla medesima linea internet del primo computer infettato. Questo virus si trasformò brevemente in un'epidemia che bloccò gli ospedali rendendo impossibile per gli operatori qualsiasi operazione elettronica. I cavi sottomarini sono

CAPITOLO 2

IL REGIME GIURIDICO DEI CAVI SOTTOMARINI

2.0 INTRODUZIONE

Una delle caratteristiche fondamentali del regime giuridico che regola il settore dei cavi sottomarini è la varietà di attori coinvolti a diverso titolo. Questa pluralità di interessi in campo genera relazioni giuridiche complesse che variano a seconda del luogo e del tipo di soggetto giuridico preso in considerazione. Ciò si deve alla natura dell'industria che, pur trattando quello che è stato definito come un "bene pubblico globale"[92], vede i privati come unici proprietari e gestori dei cavi. Tuttavia, nella costruzione di un cavo sottomarino gli Stati hanno un ruolo cruciale in quanto sono loro ad avere la giurisdizione sui punti di approdo oltre ad avere dei chiari interessi su questa infrastruttura visto l'impatto che ha sul funzionamento della società. Si mischiano interessi strategici nazionali, interessi privati e interessi dei singoli cittadini che danno vita ad un sistema giuridico stratificato e complesso. D'altronde, come si è analizzato nel primo capitolo, i cavi sottomarini sono nati grazie alla vitalità di imprenditori privati come i fratelli Brett e Cyrus Field mentre gli stati hanno sempre mantenuto un ruolo marginale specialmente dopo la stagione delle privatizzazioni delle compagnie telefoniche negli anni 80 e 90. Qui nasce il primo grande paradosso dei cavi sottomarini: un'infrastruttura essenziale

[91] Commenti di un ufficiale australiano durante la conferenza ROGUCCI.
[92] "Un interesse della società nel suo complesso, cioè un interesse che va oltre l'interesse del singolo o di semplici fazioni". Vd. A. J. Bělohlávek, "Public Policy and Public Interest in International Law and EU Law", Czech Yearbook of International Law, 2012, pp. 117-149, p. 120.

per gli stati ma completamente gestita da aziende private. Il conflitto tra l'interesse del privato (il profitto) e quello del pubblico che è un interesse non di natura esclusivamente economica, è ampio e le leggi attualmente in vigore non riescono a risanarlo. La rottura di un cavo può generare danni ben maggiori per lo stato che lo utilizza rispetto al privato che lo possiede. Inoltre, questo paradosso è alla base della difficoltà di assegnare la giurisdizione sui cavi in quanto essendo di natura privata non possiedono nazionalità, non sono riconosciuti come territorio di un paese sovrano. Il valore strategico dei cavi sottomarini ha portato gli stati a instaurare rapporti molto stretti con le proprie aziende operanti nel settore con l'obiettivo di poter ottenere un'influenza indiretta sulla morfologia di internet e sul controllo dei dati. Queste dinamiche sono rese ancor più complesse dalla mancanza di centri decisionali che fungano da enti regolatori della materia, tanto a livello internazionale quanto nazionale. Questa frammentarietà di soggetti, istituzionali e non, ha ricadute sia sul momento di elaborazione della norma che della sua applicazione in quanto non vi è chiarezza sulla giurisdizione che vige a livello internazionale sui cavi sottomarini al di fuori delle acque territoriali. L'ambito giuridico è quello che rappresenta maggiori incognite e incoerenze ma la sua comprensione è vitale per comprendere come si muovono i vari attori e quali siano le forze industriali che lo governano.

In questo capitolo si analizzeranno principalmente tre temi: il ruolo del diritto internazionale e come questo influenza i comportamenti degli Stati, il funzionamento dell'industria dei cavi sottomarini ed il ruolo dei privati, la *governance* dei cavi sottomarini ed il ruolo delle organizzazioni internazionali e regionali. Per evitare di risultare eccessivamente didascalici e ripetitivi rispetto ai numerosi lavori su questo tema, l'approccio utilizzato è quello di partire dalla fattispecie per poi capire quali siano le norme applicabili.

I cavi sottomarini sono stati oggetto di attenzione da parte del diritto internazionale fin dai suoi albori[93]. Tra il 1884 e il 1982 sono stati elaborati quattro strumenti giuridici per legiferare i cavi sottomarini: la Convenzione del 1884 per la Protezione dei Cavi Telegrafici Sottomarini ("Convenzione sui cavi del 1884"); la Convenzione di Ginevra del 1958 sull'alto mare, la Convenzione sulla Piattaforma Continentale e la Convenzione delle Nazioni Unite sul diritto del mare del 1982 ("UNCLOS"). Il primo atto venne stipulato da 48 paesi e riguardava esclusivamente la protezione dei cavi telegrafici mentre i successivi accordi internazionali hanno una portata più ampia in termini di applicabilità. Durante questa analisi, l'UNCLOS è considerato il regime attualmente applicabile per i cavi sottomarini in quanto risulta il trattato con più Stati firmatari tra quelli citati ma

[93] La regolamentazione dei cavi è stata discussa in sette conferenze internazionali tra il 1863 e 1913. Vedi *United Nations Documents on the Development and Codification of International Law*, 41 AM. Journal of International Law. Supp. 29, 33-34.

per completezza di analisi si ritiene rilevante descrivere brevemente anche le altre fonti normative che hanno dato origine all'UNCLOS e che hanno sancito alcuni principi fondamentali.

I cavi sottomarini vennero descritti come un bene essenziale per l'umanità[94], paragonabile a quello della sanità pubblica, già a partire dalla loro nascita. L'obiettivo fondamentale della Convenzione sui Cavi del 1884[95] era di esigere che gli Stati adottassero una legislazione nazionale a protezione dei cavi sottomarini che fosse applicabile nelle acque internazionali. Nonostante alcuni accordi precedenti[96], la Convenzione non si applicava in tempi di guerra e fin da allora i cavi sono rimasti obiettivi di guerra legittimi. Innanzitutto, il trattato stabiliva come reato punibile la rottura di un cavo per "negligenza colposa"[97] salvo che tale condotta non fosse dovuta al salvataggio della sua o di altre imbarcazioni[98]. La Convenzione prevedeva la possibilità di "visita in alto mare" da parte di navi da guerra straniere per raccogliere prove su eventuali illeciti nei confronti dei cavi sottomarini[99]. Tuttavia, non era prevista la possibilità di sequestrare nessun documento o arrestare il personale dell'imbarcazione. L'unica circostanza in cui venne invocato tale articolo risale al 1959 e coinvolse una nave da guerra statunitense ed il peschereccio sovietico Novorossijsk sospettato di aver rotto un cavo sottomarino nell'Atlantico[100]. Infine, la Convenzione comprendeva anche disposizioni riguardanti gli obbligo di risarcimento dei danni in caso di distruzione di un cavo preesistente durante l'operazione di posa di un nuovo cavo o tramite ancore e reti nelle operazioni di pesca[101].

La diffusione del sistema dei cavi sottomarini, il maggiore sfruttamento degli oceani e lo sviluppo delle capacità dei pescherecci richiedevano nuovi istituti giuridici volti a legiferare l'utilizzo del mare. Per tali ragioni le Nazioni Unite diedero mandato alla Commissione per il Diritto Internazionale che nel 1956 pubblicò una bozza di 73 articoli sulla legislazione internazionale del mare. Questo documento, che sarebbe poi stato utilizzato come base per l'elaborazione della Convenzione di

[94] T. Twiss, "Submarine Telegraph Cables, XLIX:XI The Nautical Magazine, pp.883-884, Novembre 1880.
[95]Convenzione per la Protezione dei Cavi Telegrafici Sottomarini 1884, adottata a Parigi il 14 marzo 1884; entrata in vigore il 1 maggio 1888.
[96]Si fa riferimento ad alcuni accordi raggiunti tra Francia, Brazile, Italia, Haiti, Portogallo nel 1864. Vedere L. Renault, The Protection of Subamrine Telegraphs and the Paris Conference, International Law Review, Merzbach and Falk, 1884.
[97] Tale terminologia, poi ripresa nei successivi trattati internazionali, si riferisce alle precauzioni richieste dall'ordinaria esperienza del marinaio e dalle particolari circostanze in cui si trova la nave in quel determinato momento.
[98] Articolo II, Convenzione per la Protezione dei Cavi Telegrafici del 1884.
[99] Ibidem, Art. 10. "Quando gli ufficiali al comando... di navi da guerra, [o di altre navi commissionate]... hanno motivo di ritenere che un'infrazione della... presente Convenzione sia stata commessa da una nave diversa da una nave da guerra, possono chiedere al capitano o al comandante la presentazione dei documenti ufficiali comprovanti la nazionalità di detta nave. (...) Inoltre, detti ufficiali potranno redigere dichiarazioni formali dei fatti, qualunque sia la nazionalità della nave incriminata.
[100] D. Guilfoyle, Tamsin Philipa Paige, R. McLaughilin, The Final Frontier of Cyberspace: The Seabed Beyond National Jurisdiction and the Protection of Submarine Cables, Cambridge University Press, 25 Luglio 2022.
[101] Art. IV e VII della Convenzione sui Cavi del 1884.

Ginevra sull'Alto Mare del 1958, ricomprendeva gli articoli II, IV e VII della precedente Convenzione sui Cavi del 1884 a cui venne aggiunto in modo esplicito il diritto di posare liberamente cavi sottomarini da parte di tutti gli Stati[102]. Questo Draft di articoli venne formalizzato all'interno di un accordo internazionale noto come la Convenzione di Ginevra sull'Alto mare del 1958[103]. Tuttavia, a causa del processo di decolonizzazione che aveva portato alla creazione di nuovi confini e dello sviluppo tecnologico ci si rese conto che fosse necessaria una nuova e più completa Convenzione. Pertanto, nel 1973 sono cominciate le trattative che diedero luce, nove anni più tardi, all'UNCLOS.

La stipula dell'UNCLOS nel 1982 ha segnato un passaggio chiave nella storia delle relazioni e del diritto internazionale. È stata spesso definita come "la Costituzione dell'Oceano" e ha richiesto nove anni di trattative per vedere la luce. Ad oggi rimane uno dei trattati più ampiamente ratificati con 168 firmatari, compresa l'UE. Lo scopo iniziale dell'UNCLOS era quello di definire le zone di giurisdizione di ciascun paese costiero sui mari ed i diritti e obblighi che ne conseguono. Queste "zone" sono: aree a sovranità territoriale (le acque interne e arcipelagiche), aree al di fuori della sovranità territoriale ma all'interno della giurisdizione nazionale (la Zona Economica Esclusiva e la Piattaforma Continentale) e le aree oltre la giurisdizione nazionale (Alto Mare e fondali marini). L'UNCLOS stabilisce importanti regole per quanto concerne l'installazione, la riparazione e la manutenzione dei cavi a seconda delle aree in cui essi si trovano. Di seguito si analizzeranno i diritti e gli obblighi in capo agli stati nelle diverse zone territoriali per poi stabilire quali responsabilità sono in capo agli Stati costieri e quali agli stati terzi.

2.1 L'INSTALLAZIONE DEI CAVI SOTTOMARINI

2.1.1 Alto mare

Il diritto di posizionare liberamente i cavi sottomarini nell'alto mare è stato sancito sia nella Convenzione sull'Alto Mare del 1958 che nell'articolo 87 dell'UNCLOS. A rinforzare il concetto interviene anche l'articolo 112 secondo cui "Tutti gli Stati hanno il diritto di posare cavi e condotte sottomarine sul fondo dell'alto mare, al di là della piattaforma continentale"[104] . Tuttavia, non si tratta di una libertà illimitata: gli Stati non devono recare danni ai cavi già posizionati e non pregiudicare

[102] Draft del Diritto del Mare della Commissione sul Diritto Internazionale, ILC, 1956, Art. 61(2) e 70.
[103] La Convenzione di Ginevra si componeva di quattro distinte convenzioni che riguardavano l'Alto Mare, Il Mare Territoriale e la Zona Contigua, la Piattaforma Continentale, la Pesca e Conservazione delle Risorse viventi nell'Alto Mare.
[104] L'articolo specifica che per i cavi posati sulla piattaforma continentale oltre i 200 mm, si applica il regime valido per la piattaforma continentale e non quello dell'Alto Mare.

le attività di riparazione di cavi già posizionati[105]. Inoltre, è necessario rispettare sempre la libertà di navigazione dell'alto mare[106].

2.1.2 La Zona Economica Esclusiva e la Piattaforma Continentale

Una delle sfide dell'UNCLOS fu quella di armonizzare il principio di libertà di posa dei cavi sottomarini nell'alto mare con i nuovi diritti degli Stati costieri nelle Zone Economiche Esclusive (ZEE) e sulla piattaforma continentale[107]. Difatti si tratta di zone sui cui gli stati costieri non vantano una sovranità territoriale ma solamente dei diritti sovrani sulle risorse e strutture che vi sono al loro interno[108]. Ad esempio, gli Stati costieri hanno il diritto di esplorazione della piattaforma continentale e di sfruttamento delle sue risorse naturali. Medesimi diritti sono previsti per la Zona Economica Esclusiva che può ricomprendere fino ad un massimo di 200 miglia nautiche dalla costa. In entrambe queste fattispecie è inviolato il diritto degli Stati di porre liberamente i cavi come previsto dall'apposito articolo 58 sulla ZEE e come ribadito anche dall'articolo 79 Parte VI[109]. Le operazioni di manutenzione e riparazione dei cavi, pur se non esplicitamente citate, sono da ritenersi comprese negli "altri usi del mare, leciti in ambito internazionale, collegati con tali libertà, come quelli associati alle operazioni di navi, aeromobili, condotte e cavi sottomarini …"[110]. Tuttavia, anche il diritto di posa dei cavi non è illimitato. Difatti è necessario porre il dovuto riguardo ai cavi già posizionati e soprattutto ai diritti che vantano gli Stati costieri nelle ZEE come la loro giurisdizione sulle ricerche scientifiche che vengono condotte in queste acque, sulla protezione dell'ambiente marino e sulle strutture e installazioni (comprese isole artificiali) presenti nell'area in questione. Infine, secondo l'articolo 58 della Convenzione, gli Stati che sono impegnati in operazioni di posa devono rispettare le leggi adottate dallo Stato costiero (conformi all'UNCLOS) e le altre leggi internazionali che non siano incompatibili con la Convenzione del 1982. Pertanto, vi sono obblighi e diritti per entrambe le parti in gioco (Stati costieri e proprietari dei cavi).

---

[105] Vedi UNCLOS, art. 79 comma 5.
[106] Id.
[107] Id, art. 76 "La piattaforma continentale di uno Stato costiero comprende il fondo e il sottosuolo delle aree sottomarine che si estendono al di là del suo mare territoriale attraverso il prolungamento naturale del suo territorio terrestre fino all'orlo esterno del margine continentale, o fino a una distanza di 200 miglia marine dalle linee di base dalle quali si misura la larghezza del mare territoriale, nel caso che l'orlo esterno del margine continentale si trovi a una distanza inferiore."
[108] Nello specifico, gli stati costieri possiedono giurisdizione sull'istituzione e utilizzo di isole artificiali, installazioni e strutture (Art. 60, 80, 87, 147, 208, 214, 246, 259), sulla ricerca scientifica marina (Artt. 87, 238-265, 297) e sulla protezione e preservazione dell'ambiente marino (Artt. 192-237).
[109] "Tutti gli Stati hanno il diritto di posare cavi e condotte sottomarine sulla piattaforma continentale, conformemente alle disposizioni del presente articolo." UNCLOS, Art. 79.
[110] UNCLOS, Art. 58 comma 1.

2.1.3 Acque Territoriali

Infine, lo Stato costiero mantiene completa giurisdizione sui cavi che si trovano nelle sue acque territoriali e questo gli consente di richiedere apposite licenze e permessi alle navi impegnate nella manutenzione e posa dei cavi. Ad ogni modo sono previste delle limitazioni anche sulle regole che gli Stati possono imporre: devono essere "misure ragionevoli"[111] e non devono danneggiare i diritti di altri Stati, specialmente per quanto concerne il diritto della libertà di navigazione come sancito nell'UNCLOS[112].

2.2 LA PROTEZIONE DEI CAVI SOTTOMARINI

La protezione dei cavi sottomarini è sempre stato un tema che ha attirato l'attenzione della comunità internazionale. Secondo l'articolo 21 dell'Unclos, gli Stati costieri hanno il diritto, ma non l'obbligo, di emanare leggi che regolino la protezione dei cavi sottomarini all'interno delle loro acque territoriali[113].

2.2.1 Acque territoriali

L'UNCLOS riconosce il diritto degli Stati costieri di adottare leggi volte alla protezione dei cavi sottomarini all'interno delle acque territoriali[114]. Queste leggi possono riguardare tanto il "passaggio inoffensivo" quanto quelle fattispecie considerate come " pregiudizievoli per la pace, il buon ordine e la sicurezza dello Stato costiero"[115]. Tuttavia, anche in questo caso l'UNCLOS non prevede l'obbligo per gli stati costieri di adottare questa normativa tanto che negli Stati Uniti è prevista una multa di appena 5000$ per il danneggiamento intenzionale di cavi sottomarini[116].

2.2.2 Acque Internazionali, Zona Economica Esclusiva e Piattaforma Continentale

Gli articoli da 113 a 115 disciplinano la protezione dei cavi nell'alto mare e sulla piattaforma continentale/ZEE. L'articolo 113 impone agli Stati di adottare dei regolamenti che riconoscano come un reato punibile il danneggiamento o la rottura di un cavo in alto mare da parte di una nave battente la sua bandiera o una persona sotto la sua giurisdizione. Tuttavia, queste leggi non devono punire le

---

[111] Si tratta di un concetto volutamente ambiguo e ampio in quanto sarebbe impossibile prevedere tutte le fattispecie che si potrebbero sorgere nell'applicazione di questo articolo. Allo stesso tempo questa ambiguità consente agli Stati costieri ampi margini di intervento nelle acque territoriali.
[112] Unclos, Art.78.
[113] Id, art. 21.
[114] Nota precedente 6, art.21, comma 1 (c).
[115] Idem, art. 19 comma 2. Tra le attività definite come pregiudizievoli per la pace vi sono gli atti di propaganda diretti a pregiudicare la sicurezza di uno stato e gli atti diretti alla raccolta di informazioni a danno della difesa dello stato costiero.
[116] Si sottolinea come l'obbligo di assumere una legislatura in materia da parte degli Stati Costieri fosse presente nella Convenzione sui Cavi del 1884. Vedi T.Davenport. (2015). Submarine cables, cybersecurity and international law: an intersectional analysis. *Catholic University Journal of Law and Technology* , pp. 83.

persone che hanno causati tali danni con l'obiettivo di salvare sé stessi o la propria nave. L'articolo 114 richiede agli Stati di adottare leggi concernenti la responsabilità dei proprietari dei cavi che, durante operazioni di posa o riparazione, danneggiano cavi già esistenti e di conseguenza sono obbligati a ripagare il danno[117]. Infine, è necessario citare l'articolo 115 secondo cui ogni Stato deve adottare leggi che garantiscano un indennizzo alle navi che subiscono danneggiamenti per evitare di danneggiare un cavo sottomarino. Questi articoli sono coniati sulla base, rispettivamente, degli articoli 2, 4 e 7 della Convenzione sui Cavi del 1884. L'articolo 113 presenta diverse limitazioni nella sua applicabilità. Innanzitutto, molti stati firmatari della convenzione non hanno ancora implementato delle sanzioni per i loro cittadini che commettono questo reato oppure le sanzioni sono ancora le stesse risalenti alla Convenzione sui cavi sottomarini del 1884 e di conseguenza le pene sono irrisorie (spesso di natura monetaria e non penale). Un altro limite è dato dall'impossibilità per gli Stati di abbordare e arrestare le navi sospettate di aver rotto intenzionalmente un cavo. L'UNCLOS è molto precisa nell'elencare le fattispecie che permettono di abbordare una nave straniera in acque internazionali[118]. Bisogna sottolineare come la Convenzione di Parigi del 1884 fosse molto più incisiva su questo argomento: l'articolo 10 prevedeva possibilità di ispezionare una nave straniera, non da guerra, imputata di aver commesso illeciti sui cavi ma senza il potere di arrestare i componenti o perquisirla[119]. Alcuni studiosi hanno ipotizzato che la fattispecie in questione possa rientrare nella definizione di pirateria contenuta all'articolo 101, lettera a), punto ii), dell'UNCLOS, da cui consegue il diritto per le navi da guerra di abbordare le navi sospettate di aver intenzionalmente danneggiato un cavo sottomarino[120]. Difatti, secondo Guilfoyle i cavi sottomarini rientrerebbero nella categoria di "beni in un luogo al di fuori della giurisdizione di qualunque stato" prevista dall'articolo 101. Perché si tratti di pirateria è necessario che l'atto non avvenga dietro ordine dell'autorità pubblica motivo per cui le navi da guerra, salvo che non siano ammutinate, non possono commettere tale reato. È bene sottolineare che non si tratta di una considerazione ampiamente condivisa nella dottrina e, secondo molti[121], è da ritenersi una forzatura dell'articolo 101. Ulteriore vuoto normativo è legato al fatto che l'UNCLOS ha giurisdizione esclusivamente sui cavi sottomarini e non anche sui landing sites e tutti gli elementi dell'infrastruttura che si trovano al di sopra dell'acqua ("dry plant").

[117] L'articolo 114 dell'Unclos si basa sull'articolo IV della Convenzione sui cavi del 1884.
[118] Nota precedente n. 6, art.110.
[119] Convenzione sui Cavi Telegrafici del 1884, Art. 10.
[120] D. Guilfoyle, T. P. (2022). THE FINAL FRONTIER OF CYBERSPACE: THE SEABED BEYOND NATIONAL JURISDICTION AND THE PROTECTION OF SUBMARINE CABLES, International e Comparative Law Quarterly, pp. 657-696.
[121] Liao, Xuexia, Protection of Submarine Cables against Acts of Terrorism. Ocean Yearbook N. 33(1), 2019, pp. 456-486.

2.3. DANNI AI CAVI SOTTOMARINI: LE RESPONSABILITA' DEGLI STATI IN TEMPO DI PACE

Nel precedente paragrafo è stata offerta una breve panoramica delle norme che regolano le differenti zone marittime istituite dall'UNCLOS. In questa sezione si intende determinare quali siano le responsabilità per gli stati che scaturiscono da suddette norme e individuare i vulnus giuridici del sistema ma anche dimostrare come alcune norme di diritto internazionale potrebbero essere applicate alle diverse fattispecie. A tale scopo si analizzeranno non più le diverse zone marittime ma le fattispecie che possono far sorgere delle responsabilità in capo agli stati.

Oltre le acque territoriali, gli sforzi normativi per determinare la responsabilità di danni ai cavi si sono concentrati sull'attribuire la giurisdizione allo stato di bandiera della nave incriminata e non agli stati costieri o utenti del cavo[122]. Questo è dimostrato dall'articolo 113 dell'Unclos (coniato dal 27 della Convenzione sull'Alto mare[123]) secondo cui gli stati devono adottare leggi che definiscano come reato punibile il danneggiamento di un cavo sottomarino ad opera di un proprio cittadino. Tuttavia, si tratta di una mera competenza prescrittiva che per essere esercitata presuppone il ritorno del cittadino sul suolo di propria competenza o, in via del tutto ipotetica e improbabile, tramite l'azione di una nave delle forze dell'ordine nei confronti di una nave mercantile battente la stessa bandiera. Risulta evidente che la simultanea presenza di questi due natanti in zone vicine ad un cavo sottomarino è assai improbabile. Il paradosso riguardante la responsabilità degli stati sui danni ai cavi sottomarini è che non è previsto l'obbligo di adottare simili regolamenti all'interno delle proprie acque territoriali o della ZEE in quanto il diritto di posa dei cavi sottomarini è riconosciuto come una libertà d'alto Mare in capo agli Stati terzi. A riguardo l'art. 79 cita un rapporto concorrenziale secondo cui lo stato costiero può adottare "misure ragionevoli per l'esplorazione della piattaforma continentale, lo sfruttamento delle sue risorse naturali e la prevenzione, riduzione e controllo dell'inquinamento provocato dalle condotte" ma senza specificare precisamente quale possa essere il contenuto di siffatti regolamenti e in ogni caso vieta la possibilità di impedire la posa o manutenzione di tali cavi e condotte. Questa ambiguità dell'UNCLOS ha dato vita a numerosi dibattiti sulla possibilità di istituire all'interno delle proprie acque territoriali o ZEE delle zone di protezione dei cavi in cui determinate attività sono vietate come realizzato da Australia e Nuova Zelanda. Il punto della questione risiede nel contenuto di tali limitazioni in quanto l'UNCLOS prevede la possibilità di imporre "termini e

[122] S. Kaye, The Protection of Platforms, Pipelines and Submarine Cables under Australian and New Zealand Law in N. Klein, J. Mossop and D Rothwell (eds), Maritime Security: International Law and Policy Perspectives from Australia and New Zealand, Routledge, 2010, pp. 186–201.

[123] A sua volta coniato dall'articolo 2 della Convenzione sui Cavi del 1884. Come già analizzato in precedenza, qualora il comandante abbia danneggiato il cavo per salvare la propria nave e incolumità dei passeggeri, non potrà essere punito.

condizioni" riguardanti la pesca nella ZEE che si applicano a tutti i paesi[124] e tali limitazioni potrebbero comprendere il divieto di pesca in determinate zone. Il regime neozelandese si applica ai propri connazionali o all'interno delle acque territoriali[125] mentre quello australiano risulta applicabile anche a cittadini stranieri e per tale ragione risulta discutibile la sua legalità a livello di diritto internazionale. Tuttavia, vi è da sottolineare come il Telecommunications Act del 1997 prevede esclusivamente sanzioni civili o ingiunzioni restrittive e non si fa alcun riferimento a norme esecutivi in acque non territoriali nei confronti di cittadini stranieri.

2.3.1 Responsabilità dello stato per danni accidentali ai cavi

Lo stato costiero non è responsabile per danni causati ai cavi nella ZEE. La domanda è se invece può uno stato essere ritenuto responsabile per danni accidentali causati da navi battenti la sua bandiera al di fuori delle proprie acque territoriali. L'articolo 113 prescrive l'obbligo di criminalizzare i propri cittadini che commettono tale reato ma non affronta il tema della responsabilità dello stato per tali danni (e di eventuali risarcimenti). Questo tema è possibile rinvenirlo nel combinato disposto degli articoli 94 e 139 dell'Unclos congiuntamente ad alcune sentenze di carattere internazionale[126][127].

La teoria che viene suggerita dagli autori del paper "The Final Frontier of Cyberspace: the Seabed Beyond National Jurisdiction and the Protection of Submarine Cables"[128] è che uno Stato abbia l'obbligo di due diligence o di prevenzione in modo da prevenire che vi possano essere danni accidentali ai cavi. Il principio in questione venne citato nell'arbitrato Trail Smelter[129] e dal Tribunale Internazionale per il diritto del Mare in due pareri consultivi e venne applicato successivamente per definire l'esistenza del "danno transfrontaliero di uno Stato"[130]. Il principio di Prevenzione si applicherebbe ai danni causati ai cavi sottomarini in quanto le navi sono considerate territorio sotto la giurisdizione dello stato di cui battono bandiera e pertanto tali Stati hanno l'obbligo di "esercitare effettivamente la propria giurisdizione e il proprio controllo in materia amministrativa, tecnica e sociale sulle navi battenti la sua bandiera"[131] in modo da evitare di essere accusati di danni transfrontalieri. La tesi che si vuole sostenere è che l'UNCLOS attribuisce la giurisdizione allo stato

[124] UNCLOS, Art. 62 comma 4. Si sottolinea come l'elenco presente in questo articolo non sia "esaustivo" ma solo un riferimento generale per gli Stati.
[125] New Zealand, Submarine Cables and Pipelines Protection Act 1996, Sezione 12-15, 1996.
[126] Richiesta di parere consultivo presentata dalla Commissione subregionale per la pesca (SRFC), caso n. 21, parere consultivo del 2 aprile 2015, ITLOS.
[127] Responsabilità e obblighi degli Stati che sponsorizzano persone ed enti rispetto alle attività nell'area, caso n. 17, parere consultivo del 1 febbraio 2011, ITLOS.
[128] Op.cit in nota 34.
[129] Caso Trail Smelter, Stati Uniti - Canada, III Reports of International Arbitral Awards, Vol. III, pp 1905- 1982, 1938.
[130] "Uno Stato è responsabile per un danno che ha origine nella sua giurisdizione ma che si realizza in un'altra giurisdizione quando ha conoscenza del danno, o mezzi per conoscerlo, e opportunità di agire". Op. cit. in nota 34.
[131] UNCLOS, Artt. 92-94.

di cui le navi incriminate battono bandiera ma allo stesso tempo, secondo il diritto internazionale consuetudinario, questi paesi possono essere responsabili di tali illeciti qualora non abbiano rispettato il principio di Prevenzione. L'ITLOS è stata consultata due volte sul tema[132] e ha stabilito come l'articolo 139 UNCLOS imponga obblighi di condotta e non di risultato sui comportamenti mantenuti dalle navi battenti la loro bandiera. In conclusione, è possibile affermare che gli Stati, per rispettare i principi sopra elencati e non essere considerati responsabili, devono non solo emanare leggi e regolamenti nei confronti delle navi su cui hanno giurisdizione volti a prevenire danni ai cavi sottomarini ma devono anche attuare un'adeguata vigilanza e controllo sui comportamenti effettivamente mantenuti dalle navi battenti la loro bandiera.

2.3.2 Danni statali o supportati dallo stato ai cavi sottomarini

Quando il danno ai cavi è causato da uno stato, l'analisi si concentra sullo *jus ad bellum* (determina quando l'utilizzo della forza è giustificato) e lo *jus in bellum* (determina come può essere combattuta una guerra). Anche in questa sezione, si analizzeranno le singole fattispecie per capire quali regimi normativi devono essere applicati e quali lacune sono presenti. Lo scopo del paragrafo è stabilire se ad un attacco cibernetico siano applicabili le stesse norme valide per un attacco armato, se i cavi sottomarini sono obiettivi militare, quali risposte possa adottare lo stato attaccato e se un attacco nei confronti dei cavi sottomarini rispetti il "criterio di proporzionalità".

I cavi sottomarini possono essere attaccati in tre modalità il cui procedimento tecnico sarà analizzato meglio nel capitolo successivo. Il primo tipo di attacco è di natura strettamente cyber e può avvenire tramite la penetrazione del Network Management System[133]. In questo modo è possibile spegnere i cavi, reindirizzarne il traffico o inserire delle backdoor al loro interno. Il secondo tipo di attacco è quello più fisico che avviene tramite la rottura del cavo stesso ed infine è possibile, tramite apposite navi, interferire con i cavi con lo scopo di estrapolare i dati al loro interno per scopi di intelligence.

2.3.3 Gli attacchi cibernetici

In letteratura non vi è una definizione univoca di cyber-attacco e spesso il termine è utilizzato in modo intercambiabile con quelli di "cyber-warfare" o "cyber-crime" sebbene le sfumature siano diverse. Il National Research Council degli Stati Uniti definisce un "Cyber Attack" come "Qualsiasi tipo di attività dannosa che tenti di raccogliere, interrompere, negare, degradare o distruggere le risorse del

[132] Sentenze citate a nota 40 e 41.
[133] Il Network Management System (NMS) è la piattaforma di gestione unificata per tutte le apparecchiature del sistema di cavi sottomarini, per gestire l'impianto umido, le apparecchiature di alimentazione elettrica (PFE), le apparecchiature di accesso ai cavi aperti (OCAE) e lo stato di funzionamento della rete durante le operazioni e la manutenzione di routine.

sistema informativo o le informazioni stesse"[134]. La definizione coniata dal Joint Chiefs of Staff statunitense è più ampia e fa rientrare tra le Computer Network Operations (CNO) anche i Computer Network Attack (CNA), i Computer Network Explorations e le Computer Network Defense (CND)[135]. Anche il glossario della NATO ha adottato la stessa terminologia ma ha aggiunto che "un attacco alla rete informatica è un tipo di cyber attacco"[136]. Per rimanere sempre nel novero delle fonti internazionali non è possibile non citare il Manuale di Tallin secondo cui "Un attacco informatico è un'operazione informatica, offensiva o difensiva, che si prevede ragionevolmente possa causare lesioni o morte a persone o danni o distruzione a oggetti"[137]. Definizione similare a quella di cyber attacco è quella di cyber crime che può essere inteso come quell'insieme di azioni commesse in violazione della legislazione internazionale e nazionale (laddove presente) che implicano l'utilizzo di computer o reti informatiche[138]. In questo senso il Consiglio D'Europa ha stilato un elenco non tassativo di alcuni crimini che possono essere considerati cyber crime come la pedopornografia e il diritto d'autore[139]. Medesime modalità sono state utilizzate dalle Nazioni Unite nel definire cosa sia un cyber crime[140] . La differenza sostanziale tra i due termini risiede nel fine ultimo dell'azione e di conseguenza anche nelle modalità: nel caso del cyber attack si mira a danneggiare l'integrità dei sistemi informatici di un paese con lo scopo di mostrarne le fragilità e metterne a rischio la sicurezza nazionale o anche con scopi difensivi qualora si voglia interrompere l'attacco che tale paese sta perpetrando mentre solitamente i cyber crimes perseguono interessi privati, quali soprattutto il guadagno economico per i loro responsabili. Secondo queste definizioni, il danneggiamento intenzionale dei cavi sottomarini o della loro infrastruttura è considerabile un cyber attacco.

Il prossimo passo è stabilire se il diritto internazionale si applica ai cyber attacchi e se offre un framework legale di protezione per i cavi sottomarini. In tal senso il dibattito è stato lungo ed ancora oggi aperto. La principale difficoltà nell'applicare il diritto internazionale al dominio cyber risiede "nella rapidità e l'anonimato dei cyberattacchi che rendono la prova della responsabilità dello Stato e

[134] National Institute of Standards and Technology - Computer Security Research Center, Defense Dictionary of Military Terms, accessibile a https://csrc.nist.gov/glossary/term/cyber_attack
[135] Chairman of the joint Chiefs of Staff, Joint Publications3.13, Information Operations, 2006.
[136] N. ATL. TREATY ORG., AAP-6, Nato Glossary of Terms and Definitions, at 2-C-12, 2008, accessibile a https://www.jcs.mil/Portals/36/Documents/Doctrine/Other_Pubs/aap6.pdf
[137] Michael N. Schmitt, Manuale di Tallin sul Diritto Internazionale applicabile alla Cyber Warfare, ed.2013, Cambridge University Press.
[138] Kulesza, Balleste, Cybersecurity and Human Rights in the Age of Cyberveillance, Rowman & Littlefield Pub Inc, 2015, pp.230, New York.
[139] Convenzione del Consiglio d' Europa sulla criminalità informatica, Budapest, 23 novembre 2001, articoli 2, 4, 5, 6, 7, 8, 9, 10
[140] The United Nations Manual on the Prevention and Control of Computer Related Crime, 1994.

distinguere tra le azioni di terroristi, criminali e Stati nazionali molto complicato"[141]. Questa fattispecie presenta le difficoltà già citate riguardanti l'individuazione del soggetto attaccante che molto spesso non è riconducibile ad uno Stato (gruppi Nation-States[142]) ma è un attore Non-Statale come nel caso di E-Crime[143] o di Hacktivist[144][145]. Naturalmente, oltre alle numerose complessità intrinseche nell'attività di attribuzione, gli analisti di intelligence devono affrontare le tattiche di deception, definite false flag[146] messe in atto dagli aggressori al fine di evitare l'associazione con gli attacchi informatici. Diversi esperti, quali il Gruppo di esperti Governativi delle Nazioni Unite e il Consulente Legale del Dipartimento di Stato americano, hanno affermato che i principi del diritto internazionale sono applicabili al dominio Cyber[147] [148].

Qualora l'attacco cyber fosse considerato al pari di un attacco armato, è necessario capire quali potrebbero essere le legittime risposte da parte dello stato attaccato. Per addentrarci al meglio nella materia è necessario capire quando i paesi hanno il diritto ad usare la forza nelle loro relazioni con gli altri paesi. Questa fattispecie è prevista dall'articolo 39 (in combinato disposto con l'articolo 42) e dall'articolo 51 della Carta delle Nazioni Unite. Nel primo caso si fa riferimento alla possibilità che il Consiglio di Sicurezza "accerti l'esistenza di una minaccia alla pace o di un atto di aggressione" e decida misure adeguate (Art. 41 e 42) per "mantenere o ristabilire la pace e la sicurezza internazionale"[149]. L'articolo 51 sottolinea il diritto di autodifesa, individuale o collettiva, che può essere esercitato da uno Stato Membro in seguito ad un attacco subito anche qualora il Consiglio di Sicurezza non abbia deliberato nessuna misura. Quindi, in linea teorica, il danneggiamento o

[141] Scott J. Shackelford & Richard B. Andres, State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem, 42 Geopolitical Journal of International Law 974(2010).
[142] Entità che lavorano per il governo o i militari di uno Stato o che operano sotto la loro direzione il cui obiettivo principale è lo spionaggio, furto o qualsiasi altra attività che favorisca gli interessi di un particolare gruppo nazionale e gli obiettivi tipici sono aziende ed organizzazioni governative.
[143] Un'organizzazione (anche individuale) in grado di condurre un'attività criminale significativa e su larga scala a scopo di lucro ed il cui scopo principale è il guadagno economico ai danni delle aziende o privati.
[144] sostenitori, altamente motivati e potenzialmente distruttivi, di cause sociali (ad esempio, commercio, lavoro, ambiente, ecc.) o di ambiti politici che tenta di annientare il modello di business di un'organizzazione o di danneggiarne l'immagine.
[145] Le definizioni delle note 35, 36 e 37 sono tratte dal sito https://www.ictsecuritymagazine.com/articoli/relazioni-tra-state-nation-ed-ecrime-actor/ e fanno riferimento alla categorizzazione utilizzata nel MISP Galaxy che è un apposito database open source in materia di intelligence e cyber threat.
[146] Si tratta di operazioni generalmente condotte nello spazio cibernetico che vengono poste in essere utilizzando cautele e tecniche tali da indurre il target a ritenere che le stesse siano riconducibili ad un attore diverso da quello che ha condotto l'attacco.
[147] U.N. Secretary-General, Developments In the Field of Information and Telecommunications In the Context of International Security, U.N. Doc. A/66/152, pp. 35-37, Giugno 11, 2011.
[148] Harold Koh, U.S. Deputy of State, Remarks at the USCYBERCOM InterAgency Legal Conference, 18 Settembre 2012, accessibile a http://www.state.gov/s/l/releases/renarks/197924.htm
[149] Art. 39: "Il Consiglio di Sicurezza accerta l'esistenza di una minaccia alla pace, di una violazione della pace, o di un atto di aggressione, e fa raccomandazione o decide quali misure debbano essere prese in conformità agli articoli 41 e 42 per mantenere o ristabilire la pace e la sicurezza internazionale", Carta delle Nazioni Unite, San Francisco, 1945.

l'interferenza intenzionale con il sistema dei cavi sottomarini potrebbe dar luogo all'uso della forza da parte dello Stato colpito nel caso in cui fosse considerato un "attacco armato" come previsto nell'articolo 51 o come una "minaccia alla sicurezza internazionale" come stabilito nell'articolo 39. L'applicazione dell'articolo 39 dipende dalle decisioni del Consiglio di Sicurezza che spesso non agisce sulla base di ragioni strettamente giuridiche ma soprattutto di carattere geopolitico. Come sottolineato da Österdahl, "il Consiglio di Sicurezza può sostanzialmente decidere o fare tutto ciò che desidera e rimarrà entro i limiti del quadro giuridico per la sua azione"[150]. Viceversa, Paige ha individuato i presupposti affinché i membri del Consiglio di Sicurezza potrebbero applicare l'articolo 39 nel caso di un taglio dei cavi sottomarini sulla base dei loro comportamenti storici[151]. Il primo elemento, che è anche quello più ovvio e facile da dimostrare, consiste nell'accertare che il taglio ai cavi rappresenti una "minaccia alla pace" tale da richiedere un intervento. Visto il ruolo che ricoprono oggi i cavi sottomarini nelle nostre società, la risposta è positiva. Il secondo presupposto è che le azioni proposte dal Consiglio di Sicurezza rientrino nel suo mandato, che sostengano i diritti all'autodeterminazione e alla non ingerenza negli affari interni ed infine che si concentrano sulla generazione di un risultato pacifico e non sul cambio di regime. Di questi presupposti, il terzo risulta il più complicato viste le dinamiche interne al Consiglio di Sicurezza e la mancanza di fiducia che vige tra i singoli paesi. Per quanto riguarda l'articolo 51, il punto principale è stabilire se il taglio ai cavi o un attacco al Network Management System siano assimilabili ad un attacco armato. Come si analizzerà successivamente, il diritto internazionale non ha ancora dato risposte univoche sul tema. La fonte più autorevole e recente è il Manuale di Tallin 2.0 secondo cui un attacco cibernetico deve essere paragonato ad uno armato sulla base degli effetti che produce (la loro durata, l'intensità, la legittimità, l'immediatezza, l'invasività)[152]. Infine, pur considerando l'attacco ai cavi sottomarini al livello di un attacco armato, la risposta del soggetto attaccato deve rispondere ai principi di proporzionalità e necessità del diritto internazionale consuetudinario.

2.3.4 Il taglio di un cavo sottomarino e il diritto dei conflitti armati

Come anticipato, i cavi sottomarini per le telecomunicazioni possono essere letteralmente tagliati in modo da interrompere le comunicazioni del nemico. Si tratta di un metodo più tradizionale e per questo la fattispecie in esame è stata oggetto di analisi fin dagli albori della storia dei cavi telegrafici. Nell'agosto 1914, uno dei primi atti di ostilità della Gran Bretagna contro la Germania fu il taglio dei

[150] Osterdahl Inger, Threat to the Peace: The Interpretation by the Security Council of Article 39 of the UN Charter,Uppsala University Swedish Institute of International Law, p. 103, 1998.
[151] TP. Paige, Petulant and Contrary: Approaches by the Permanent Five Members of the UN Security Council to the Concept of "Threat to the Peace" under Article 39 of the UN Charter, Brill, 2019.
[152] Si fa riferimento al cd. "scale and effects test". Vedi OA Hathaway et al., The Law of Cyber-Attack, California Law Review 817, pp.847–848, 2012.

cavi di comunicazione sottomarini tedeschi. Ciò non solo ha ridotto l'accesso tedesco alle infrastrutture di comunicazione ma facilitò l'intercettazione del traffico tedesco deviato. La Convenzione di Parigi del 1884 stabiliva all'articolo 15 che le sue disposizioni non si applicassero in tempo di guerra e che quindi i cavi telegrafici fossero considerabili obiettivi militari legittimi. L'Istituto per il diritto internazionale, nella sessione di Bruxelles del 1902, approvò un'importante risoluzione sul trattamento dei cavi durante la guerra che sanciva delle regole di ingaggio dei cavi sulla base della loro posizione geografica e quindi del loro status territoriale[153]. Nel tentativo di fornire ulteriori indicazioni, l'Oxford Manual of the Laws of Naval War del 1913 propose una regola più dettagliata, seguendo in gran parte l'approccio dell'Institute for International Law del 1902. In sostanza sosteneva, come anche l'articolo 54 dei Regolamenti dell'Aja del 1907, che: "il collegamento dei territori dei due belligeranti", o parti del territorio di un belligerante, potessero essere presi di mira al di fuori delle acque neutrali; un "cavo che collega un territorio neutrale con il territorio di uno dei belligeranti" potrebbe essere tagliato solo dove strettamente necessario ed entro un limite di tre miglia dalla costa belligerante o in alto mare in condizioni di blocco e che lo status dei cavi non è influenzato dalla nazionalità dei loro proprietari. Tuttavia, la norma "riconosce... che i cavi o le condutture che servono esclusivamente uno o più belligeranti potrebbero essere obiettivi militari legittimi". Pertanto, l'elemento fondamentale che venne aggiunto era il criterio di "estrema necessità di guerra" che venne anche confermato in diversi manuali navali statunitensi[154]. Le Convenzioni successive tra cui L'UNCLOS ed il Trattato sui Fondali Marini del 1971 non hanno fornito un quadro chiaro su come dovessero essere trattati i cavi sottomarini alla luce del Diritto dei Conflitti Armati. Sulla base di queste fonti, la conclusione da trarre è che il taglio in alto mare dei cavi che collegano un paese belligerante e un paese neutrale è consentito purché il cavo sia diventato un obiettivo militare (allo stesso modo in cui una nave mercantile delinquente diventa un obiettivo militare se viene impiegato a vantaggio militare dall'avversario). Questa è la visione di lunga data degli Stati Uniti e del Regno Unito nonché la logica alla base, tra l'altro, dell'approccio del Manuale di Tallinn 2.0[155].

[153] 1) che i cavi che collegano due territori neutrali siano "inviolabili"; che i cavi che collegano due belligeranti o due parti del territorio di un belligerante possono essere tagliati ovunque tranne che in acque neutrali e che i cavi che collegano un belligerante con un paese neutrale possono essere tagliati nel mare territoriale del belligerante e, se è in atto un blocco, anche in alto mare. Vedi Istituto di diritto internazionale, Câbles sous-marins en temps de guerre, Risoluzione, 23 settembre 1902, Sessione di Bruxelles. https://www.idi-iil.org/app/uploads/2017/06/1902_brux_01_fr.pdf.

[154] Art. 40, Istruzioni per la Marina degli Stati Uniti che governano la guerra marittima, 30 giugno 1917.

[155] Art. 150, paragrafo 5, M. Schmitt, Tallinn Manual on the International Law Applicable to Cyber Warfare 2.0, Cambridge University Press, 2017.

I cavi sottomarini rappresentano sia capacità militari, sia vulnerabilità militari, al di là del loro ruolo primario di conduttori di dati. Si tratta quindi di classiche infrastrutture "a duplice uso" che possono potenzialmente essere un "oggetto civile" o un "obiettivo militare"[156]. Esempi di strutture "dual use" che sono state considerate obiettivi militari legittimi sono le stazioni radiotelevisive irachene che venivano utilizzate sia con scopi di propaganda (scopo civile) sia come centri di comando e controllo militari[157]. Per tali ragioni risulta difficile considerare i cavi dei beni neutri, di natura civile e tantomeno è possibile determinare se un cavo sia utilizzato esclusivamente da un paese neutro invece che da uno belligerante. In una certa misura, quindi, questa è in realtà la domanda a cui è più facile rispondere: sì, i cavi sottomarini possono essere oggetti militari; quindi, la domanda più impegnativa è quella finale: un attacco a un cavo per le comunicazioni sottomarino non potrebbe mai essere sproporzionato?

L'approccio dottrinale alla proporzionalità si concentra sul linguaggio dell'articolo 57, paragrafo 2, lettera a), punto iii del Protocollo Aggiuntivo I (API)[158]. Dato che il taglio dei cavi sottomarini può, tra l'altro, inibire le comunicazioni e fermare le attività degli UAV[159], è chiaro che possono dare "un contributo efficace all'azione militare" e potrebbero costituire obiettivi militari legittimi. La questione fondamentale è capire se l'attacco ai cavi arrecherebbe delle vittime umane o danni eccessivi rispetto al vantaggio militare prevedibile. Si suggerisce che qualsiasi applicazione di questo test darà sempre esito negativo. Questo perché la combinazione della portata dell'impatto sulle infrastrutture civili, sociali ed economiche e la probabilità che questo danno si diffonda oltre lo Stato preso di mira fino a raggiungere Stati terzi neutrali, porta a pensare che un simile attacco potrebbe essere eccessivo rispetto a qualsiasi vantaggio militare. Si tratta di un'azione che potrebbe bloccare l'intero sistema di messaggistica vocale e scritta, diminuire fortemente le capacità di operare degli ospedali e delle infrastrutture logistiche di un paese solo per fare alcuni esempi. Inoltre, il livello di ridondanza di cui dispongono molti stati renderebbe facile il reindirizzamento delle comunicazioni militari classificate ma più complicato per le comunicazioni civili e questo è un ulteriore elemento che renderebbe

[156] "gli obiettivi militari sono limitati a quei beni che per la loro natura, ubicazione, destinazione o utilizzo apportano un contributo efficace all'azione militare e la cui distruzione, cattura o neutralizzazione totale o parziale, nelle circostanze del momento, offre un vantaggio militare definito". Manuale di Sanremo, Regola 40, 1977 Protocollo addizionale, I art 52(2);

[157] Giulio Bartolini, Air Operations against Iraq (1991 and 2003), in The Law of Air Warfare, Eleven International Publishing, 2006, Utrecht.

[158] "Il belligerante dovrebbe astenersi dal decidere di lanciare qualsiasi attacco che possa causare perdite accidentali di vite umane, lesioni a civili, danni a beni civili, o una combinazione di questi, che sarebbe eccessivo rispetto al vantaggio militare concreto e diretto previsto".

[159] Noah Schactman, "CIA Chief: Drones 'Only Game in Town' for Stopping Al Qaeda," Wired Magazine, May 19, 2009. Accessed at http://www.wired.com/dangerroom/2009/05/cia-chiefdrones-only-game-in-town-for-stopping-al-qaeda/#ixzz0e8GDppPM.

l'attacco sproporzionato. Pertanto, si conclude che il taglio dei cavi dati sottomarini, sebbene teoricamente consentito dalla LOAC e dalla legge sulla guerra navale, è funzionalmente illegale.

2.4 SOGGETTI PUBBLICI E PRIVATI

Innanzitutto, è necessario distinguere i soggetti privati sulla base del ruolo che possiedono nel processo di costruzione di un cavo sottomarino. Solitamente chi possiede il cavo commissiona le opere di costruzione, installazione e manutenzione del cavo ad altri soggetti che sono i fornitori. Quest'ultimi possono essere divisi in tre gruppi: il primo, nonché il principale, è composto da aziende che sono in grado di ideare, realizzare e installare tutti i componenti di un cavo sottomarino. Un secondo gruppo di aziende è quello incaricato di incrementare la capacità di trasmissione[160] di un cavo cambiandone la tecnologia obsoleta con quella più moderna. Infine, vi sono le società che fabbricano il cavo sottomarino ma non realizzano la posa in mare. Il mercato dei fornitori è dominato da poche aziende[161]. Per quanto riguarda le società che fabbricano e talvolta installano il cavo vi sono quattro aziende principali: Alcatel Submarine Network, di proprietà di Nokia, Subcom, produttore e installatore di cavi statunitense, NEC, multinazionale giapponese dell'informatica[162], e infine HMN, ex Huawei Marine Network che è fortemente influenzata dalla Cina. Per quanto riguarda gli installatori, le aziende principali sono Subcom e Alcatel, Orange Marine con sede in Francia ma operante soprattutto in Spagna e Nord Africa[163] e Global Marine Systems con sede in Gran Bretagna. Come si vedrà nel capitolo successivo, i fornitori ricoprono un ruolo delicatissimo in quanto, tramite la gestione dei landing sites e la fabbricazione del cavo stesso, sono i soggetti che più facilmente possono inserire backdoor all'interno del sistema. Questa preoccupazione è stata condivisa anche dal governo statunitense come dimostrato dalla decisione del presidente Biden e della Federal Communications Commission (FCC) di vietare la futura vendita di servizi o apparecchiature di Huawei Marine negli Stati Uniti[164]. Menzione a parte, nella catena del valore, meritano i provider dei

[160] Ci si riferisce alla capacità massima di dati al secondo che possono essere trasmessi attraverso il cavo. Negli ultimi 30 anni si è passati da cavi come il Global Cloud Xchange's FLAG Europe Asia installato nel 1997 che trasportava 500 gigabit al secondo a cavi come il MAREA che trasporta 200 terabit al secondo. Per contestualizzare questo dato, un cavo contenente solo otto fili di fibre ottiche avrebbe una capacità sufficiente per trasferire l'intero contenuto della della Bodleian Library attraverso l'Atlantico in circa 40 minuti. Vd. J. Kim, Submarine Cables: the Invisible Fiber Link Enabling the internet, Dgtl Infra, 4 Maggio 2022. Submarine Cables: the Invisible Fiber Link Enabling the Internet - Dgtl Infra

[161] id.

[162] J. Hillman, Securing the Subsea Network: a Primer for Policymakers, CSIS, Marzo 2021.

[163] C. Bueger, T. Liebetrau e J. Franken, Security Threats to Undersea Communications Cables and Infrastructure: Consequences for the EU, Sottocommissione del Parlamento Europeo per la Sicurezza e Difesa, giugno 2022, p.38.

[164] FCC bans equipment Authorizations for Chinese Telecommunications and Video Surveillance Equipment Deemed to Pose a Threat to National Security, Federal Communications Commission, 25 Novembre 2022, Accessibile a DOC-389524A1.pdf (fcc.gov)

servizi più strettamente "marittimi", che forniscono le imbarcazioni e il personale specializzato per la messa a fondo dei cavi sulla base dei cosiddetti Zone Cable Maintenance Agreements[165].

2.4.1 Modelli Commerciali

Per quanto riguarda il modello proprietario, vi sono due principali tipologie. Il più comune in assoluto è il modello rappresentato dal consorzio. Questa soluzione prevede un raggruppamento di imprese che mette in comune le risorse per la costruzione del cavo, condividendone la capacità di trasmissione. Ciascuna azienda dispone di un determinato volume di capacità del cavo che può scegliere di utilizzare per sé o vendere sul mercato all'ingrosso. Il volume di capacità assegnato a ciascun membro del consorzio non è sempre proporzionato ai livelli di investimento individuali[166]. Quest'ultimi possono dipendere dal fatto che il membro del consorzio sia una parte di approdo all'estremità del cavo, una parte di approdo all'estremità di una diramazione o una parte non di approdo. La capacità complessiva di un cavo viene suddivisa tra una parte che rimane non utilizzata e di proprietà del consorzio[167] ed una parte che viene suddivisa tra i vari membri. Questi possono decidere a loro volta di utilizzarla autonomamente o di affittarla ad altre compagnie per un determinato tempo (solitamente per 25 anni che è la durata di vita dei cavi)[168]. In questa fattispecie, l'azienda che "affitta" il cavo non ha potere decisionale sulla gestione dell'infrastruttura in quanto non ha partecipato all'investimento iniziale. Pertanto, si utilizza circa il 20% della capacità complessiva di un cavo[169].

I rapporti tra i singoli membri del consorzio, i diritti di ciascuna azienda ed i dettagli sulla gestione del cavo sottomarino sono disciplinati dal Construction and Maintenance Agreement (C&MA). Sempre all'interno di questo documento è descritta la governance del consorzio che solitamente prevede un consiglio (Management Committee) composto dai rappresentanti delle varie aziende all'interno del quale vengono prese le decisioni più rilevanti e poi una serie di sotto commissioni che supportano il Management Committee sui diversi aspetti inerenti la vita del cavo.

Un altro modello di business è quello dei "cavi privati", che hanno come primo obiettivo il mercato all'ingrosso e la rivendita di capacità piuttosto che l'utilizzo personale. In questo modello possono anche agire uno o più investitori istituzionali (come, ad esempio, fondi sovrani). Reverdy e Skenderoski[170] definiscono gli abituali requisiti di finanziamento per la costruzione di cavi

[165] Vd. Capitolo 1.3.2 dell'elaborato.
[166] M. Green, The Submarine Cable Industry: How Does it work?, contenuto in "Submarine Cables: the Handbook of Law and Policy, 2013, pp. 48.
[167]Ci si riferisce alla cosiddetta Common Reserve Capacity che viene utilizzata dal consorzio qualora vi fosse l'esigenza di reindirizzare parte del traffico sul cavo in questione per via di danni subiti da altri cavi del consorzio.
[168] Op. cit. nota 165.
[169] Ibidem.
[170] D. Reverdy, & I. Skenderoski, Submarine Cables: Structuring and Financing Options. Salience Consulting

sottomarini a fronte di investimenti corposi in capitale fisso (CAPEX[171]) comparati con una spesa operativa (OPEX) nettamente minore (in media appena il 6% del CAPEX), che viene più che finanziata dai flussi di cassa derivanti dall'eventuale vendita di capacità. Negli ultimi anni si è assistito ad una forte espansione di questo modello societario ma per un utilizzo personale rispetto che alla vendita all'ingrosso. Questo fenomeno si deve all'ingresso nel mercato delle grandi aziende tech come Google, Meta, Microsoft che necessitano di connessioni con alti standard tecnologici e preferiscono costruire cavi sulla base delle loro necessità. Inoltre, il modello single owner si è affermato anche grazie alla riduzione dei costi di produzione[172] e al vantaggio di poter prendere decisioni strategiche sul cavo senza doverle concordare con le altre aziende come nel caso del consorzio. Questo cambiamento da parte degli OTT sta mettendo in crisi gli operatori delle telecomunicazioni e tutte quelle aziende il cui core business era la vendita all'ingrosso oltre a destare diverse preoccupazioni di natura geopolitica. Il punto è stato centrato dal giornalista Christopher Mims: "immaginiamo se Amazon possedesse le strade su cui consegna i suoi pacchi".

2.4.2 Metodi di finanziamento

Per far fronte all'ingente finanziamento iniziale che richiede la costruzione di un cavo[173], le aziende private possono ricorrere a diversi metodi che dipendono dalla presenza di un singolo proprietario o di più proprietari. In quest'ultimo caso, il consorzio si avvale dell'autofinanziamento delle aziende partecipanti e quindi non sono presenti particolari finanziamenti esterni. Discorso diverso vale per i cavi privati per i quali il metodo più comune consiste nella pre-vendita della capacità di trasmissione in modo da essere sicuri degli introiti che si avranno appena completata l'infrastruttura. Un altro metodo è quello di istituire un'azienda nuova ma con il capitale messo a disposizione da diverse società; in questo caso l'unica differenza con il consorzio risiede nel fatto che le risorse non rimangono in mano agli operatori di telecomunicazioni ma saranno di proprietà di questa nuova azienda. Un'alternativa al cavo privato prevede che le aziende, invece di impegnarsi direttamente, possano cimentarsi nella creazione congiunta di società di progetto (Special Purpose Vehicles) per la partecipazione al progetto[174]. In tal modo, il finanziamento è reso più agevole al prezzo, però, di una

White Paper, 2015. Accessibile a https://salienceconsulting.ae/wpcontent/uploads/2018/09/Submarine_Cables_Structuring_and_Financing_Options_Jan_2015.pdf

[171] Capital Expenditures (CAPEX) rappresentano flussi di cassa in uscita per la realizzazione di investimenti in attività immobilizzate di natura operativa. Si tratta cioè di investimenti in capitale fisso.

[172] Questo fenomeno si deve agli sviluppi tecnologici che oggi permettono di inviare più lunghezze d'onda ottiche tramite una singola coppia di fibre. Per approfondire vedi capitolo 1.

[173] Si passa da cavi come FASTER di Google dal costo di 300 milioni di euro a cavi come il 2Africa, il più lungo al mondo, che è costato più di un miliardo di euro. Vd. M. Zhang, Equinix Brings 2Africa Subsea Cable to Genoa and Milan, Dgtl Infra, 24 febraio 2021, Accessibile a https://dgtlinfra.com/equinix-2africa-subsea-cable-genoa-milan/

[174] Vd. Nota 74, pp.50.

minore autonomia nel management dell'infrastruttura in quanto le imprese che compongono l'SPV non avranno potere decisionale. In entrambi i casi ci si può avvalere dei prestiti delle banche di sviluppo (MDB) che presentano tassi di interesse più bassi delle banche commerciali. Il 90% degli investimenti complessivi in cavi sottomarini tra il 1990 ed il 2020 è stato effettuato da sistemi a più proprietari ma se si prende in considerazione il periodo 2016-2020 si osserva una forte inversione di tendenza: i sistemi a proprietario singolo rappresentano il 28% e gli MDB l'11% rispetto al 61% dei sistemi a proprietario multiplo[175].

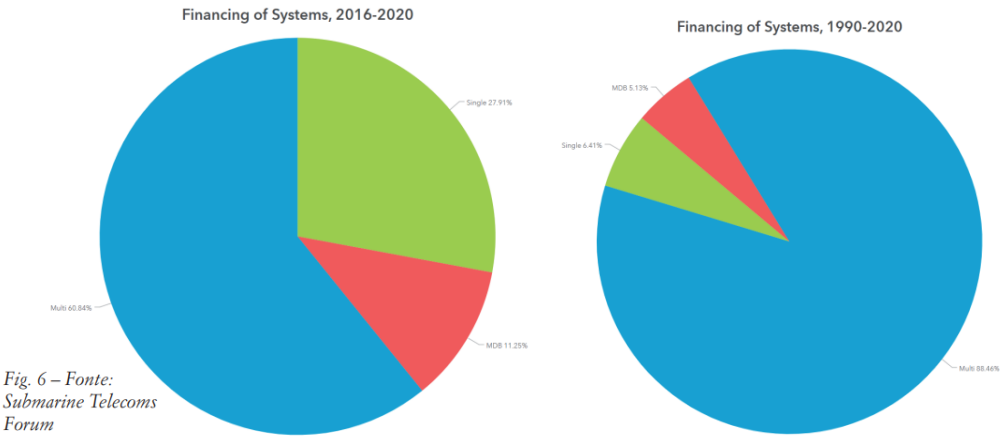


Fig. 6 – Fonte: Submarine Telecoms Forum

Figura 10 e 3: V. Francola, AM Mensah, L'industria dei cavi sottomarini, qualche elemento introduttivo, Astrid

2.4.3 Tipologie di aziende

Le aziende che operano in questo settore si differenziano sulla base di due caratteristiche fondamentali: il loro profilo aziendale e il loro status giuridico.

Sebbene gli Stati non controllino direttamente i cavi possono possedere importanti quote azionarie in alcune aziende. Questo fenomeno è tipico dei paesi dove il potere statale è maggiore come nel caso della "China Unicom"[176] che è completamente di proprietà della Repubblica Popolare Cinese o di TeleYemen che è anch'essa posseduta dallo stato yemenita. Tuttavia questo tipo di aziende, seppur in aumento, sono minoritarie rispetto a quelle controllate solamente da privati.

[175] V. Francola, Gordon A. Mensah, L'industria dei cavi sottomarini: qualche elemento introduttivo, Astrid Rassegna (Laboratorio sull'Ecosistema Digitale Astrid).
[176] Il nome legale della società è "United Network Communications Group C., Ltd".

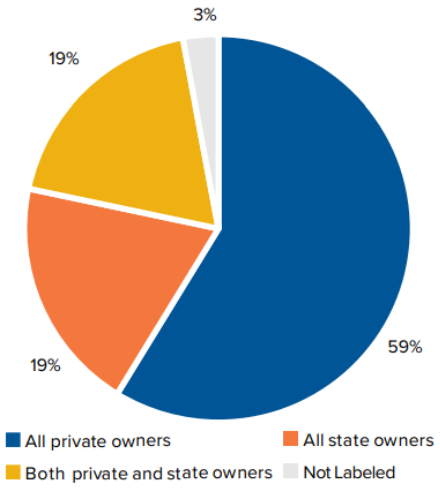


Figura 11: Ripartizione della proprietà pubblico-privata dei cavi.

Fonte: J. Sherman, Cyberdefence across the ocean floor, Scowcroft Center for Strategy and Security, settembre 2021, pp.9.

La maggior parte delle aziende che gestiscono i cavi sottomarini sono di proprietà di azionisti privati. In questo caso si possono avere cavi gestiti da una singola azienda oppure da consorzi di aziende come nel caso del cavo "Asia Africa Europe-1 (AAE-1)" che è uno dei più lunghi al mondo ed è posseduto da oltre 15 aziende. Questo è un fenomeno tipico dei cavi che devono passare per diversi paesi e quindi diverse giurisdizioni. Infine, vi sono aziende che prevedono una partecipazione azionaria da parte dello stato ma in misura non maggioritaria e pertanto non controllano la società. Questo è il caso di Rostelecom, il più grande vettore di telecomunicazioni russo, che è partecipata dall'Agenzia federale per la gestione della proprietà statale (Rosimushchestvo) al 35,91% delle azioni. In queste fattispecie lo Stato non ha il potere formale di prendere le decisioni in modo autonomo ma ha un forte potere persuasivo in special modo nei paesi autoritari dove tali aziende devono rispondere al potere politico e agli interessi dello stato.

Altro elemento interessante da indagare è la tipologia di azienda che posa o possiede i cavi sottomarini. Gli operatori di telecomunicazioni sono il tipo di azienda più diffusa nel settore e possono esistere sotto forma di qualsiasi entità giuridica a seconda della giurisdizione in cui hanno la sede legale. Pertanto, i cavi sottomarini possono essere posseduti da Public Company Limited by Shares come nel caso di Vodafone che è una delle maggiori società di telecomunicazioni del Regno Unito. A loro volta le aziende madri possiedono diverse filiali che gestiscono una parte dei loro cavi per quanto concerne le operazioni di posa e manutenzione come nel caso della Orange Marine che è invece una

Società per azioni semplificata[177] . Pertanto, anche per quanto riguarda la natura giuridica dei proprietari e gestori dei cavi vi è un'ampia varietà.

Negli ultimi anni si è assistito all'ingresso nel settore di aziende diverse rispetto agli operatori di telecomunicazioni. Difatti i cosiddetti OTT (Over-The-Top)[178] stanno rivoluzionando il mercato con la scelta di costruire l'infrastruttura di internet autonomamente e non dipendere più dagli operatori[179]. Ciò che più sorprende è che si tratta di un mercato che attrae investimenti da parte anche di società che non hanno esigenza diretta di possedere un cavo come nel caso del Loret Group[180] che è proprietaria del cavo sottomarino Global Carribean Network (GCN). Infine vi sono le banche di investimento che possono anche possedere capacità in un cavo come garanzia per il finanziamento del debito fornito ad un'azienda per il completamento del cavo.

2.5 LE TENDENZE DEL MERCATO

Il mercato dei cavi sottomarini ha raggiunto una dimensione del mercato pari a 17.18 miliardi di dollari nel 2023 e secondo le previsioni dovrebbe arrivare ad una quota di 41 miliardi entro il 2032[181]. Ad oggi si contano 552 cavi attivi o pianificati che connettono tutti i continenti ad eccezione dell'Antartide[182]. La crescita è destinata ad aumentare per diverse ragioni, tra cui l'aumento dell'utilizzo dei cloud services ed in generale la domanda di banda larga a livello globale che si raddoppia ogni due anni[183]. Questi dati si riscontrano sia nei livelli di investimento che, solo nel periodo 2017-2021, ammontano a 9,2 miliardi ma anche nel numero di cavi che vengono installati o pianificati. Il periodo 2016-2020 ha registrato in media una messa in posa di circa 67.000 chilometri aggiunti ogni anno mentre si stima che, nel triennio 2022-2024, i chilometri aggiuntivi saranno, rispettivamente, nell'ordine di 120.000, 103.000 e 116.000[184].

---

[177] "Le principali caratteristiche sono una grande duttilità di funzionamento e la possibilità per i soci di regolamentare negli statuti le condizioni per diventare soci e per recedere dalla società". Nel sistema giuridico inglese assume il nome di "simplified joint-stock company". Vd. https://ascheri.co.uk/francia-la-societa-per-azioni-semplificata/#:~:text=La%20SAS%2C%20societ%C3%A0%20per%20azioni,pu%C3%B2%20ricorrere%20al%20pubblico%20risparmio.

[178] Con l'espressione OTT - TV si fa riferimento a quelle piattaforme televisive o audiovisive gestite da società i cui servizi sono primariamente veicolati attraverso infrastrutture di rete di terzi e che, in tal senso, agiscono al di sopra (over-the-top) delle reti.

[179] Submarine Telecoms Forum, Inc., Submarine Telecoms Industry Report: 2020/2021 Edition, October 23, 2020, Accessible a https://subtelforum.com/products/ submarine-telecoms-industry-report/.

[180] L'azienda in questione opera nel noleggio di auto e i servizi di leasing.

[181] Precedence Research, Submarine Cable System Market, 2023, Accessibile a https://www.precedenceresearch.com/submarine-cable-system-market .

[182] TeleGeography, Submarine Cable FAQ, 2023, Accessibile a https://www2.telegeography.com/submarine-cable-faqsfrequently-asked-questions.

[183] Op. Cit, V. Francola, Gordon A. Mensah, L'industria dei cavi sottomarini: qualche elemento introduttivo, pp. 4.

[184] Ivi, pp. 22.

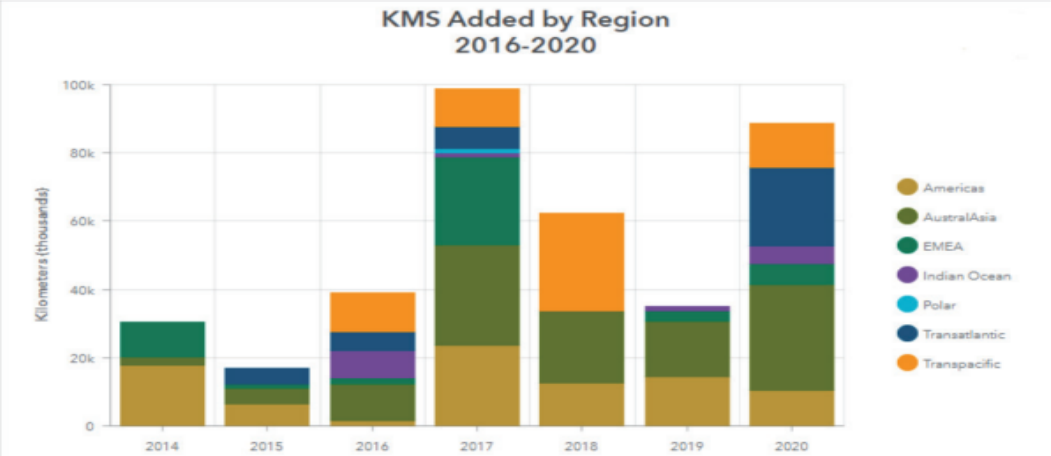


Figura 12: Chilometri di cavi sottomarini costruiti per regione.

Fonte: V. Francola, Gordon A. Mensah, L'Industria dei cavi sottomarini: qualche elemento introduttivo, Astrid, 2021, pp.22

Geograficamente, l'Asia Pacifico continua a dominare il mercato globale ma con importanti sviluppi regionali dettati soprattutto dalle esigenze degli operatori OTT di collegare non più le città ma i loro data center. La rotta più competitiva rimane quella che unisce Londra a New York ma si assiste alla nascita di rotte inedite da Virginia Beach alla Francia o dal Brasile all'Africa. Questo si lega alla crescita esponenziale nella domanda che sta vivendo sia il continente africano, dove pur vivendo il 17% della popolazione mondiale vi si trova solo l'1% dei data center globali, sia il Sud America dove il Cile si propone come il principale connettore con i mercati asiatici[185]. Lo sviluppo di questi mercati è dimostrato anche dai dati della Banca Mondiale secondo cui la crescita del 10% della copertura di banda larga in un paese a basso-medio reddito può portare ad un aumento del 1,38 del Prodotto Interno Lordo[186]. Esempi di questo trend sono il cavo Equiano che parte dall'Europa per arrivare fino al Sud Africa ed il cavo 2Africa, il più lungo al mondo, che attraversa ben 33 paesi. In entrambi i progetti vi è la partecipazione di Google.

Il mercato sembra fortemente influenzato dalle scelte di investimento degli operatori OTT. Basti pensare che Microsoft, Google, Amazon e Meta oggi possiedono il 69% della capacità globale di trasmissione[187]. Sono i leader di mercato sia dal punto di vista del numero che della lunghezza dei cavi posseduti con una quota di mercato pari al 53%[188]. I principali Content Providers rimarranno Google, Facebook (Meta), Microsoft e Amazon con quest'ultima che vedrà un forte aumento degli

[185] Op. Cit. a nota 70, J. Hillman.
[186] N. Gelvanovska, M. Rogy, and Carlo Maria Rossotto, Broadband Networks in the Middle East and North Africa Accelerating High-Speed Internet Access, Banca Mondiale, 2014.
[187] Sydney, Brooke, Pleasic, Securing Subsea Cable Critical Infrastructure, Holes in the Governing Legal Framework in the United States and Internationally, Seton Hall University, 2024
[188] Dal calcolo sono escluse le aziende che hanno pianificato meno di tre cavi nei prossimi 5 anni. Vedi PWC, Study to Monitor Connectivity – Connecting the Eu to its partners through submarine cables, European Commission, 2022.

investimenti mentre la società di Mark Zuckerberg diventerà l'azienda leader. Le aree geografiche in cui saranno installati più cavi sono quella del Transpacifico (10) e l'EMEA con importanti risvolti per l'Unione Europea.

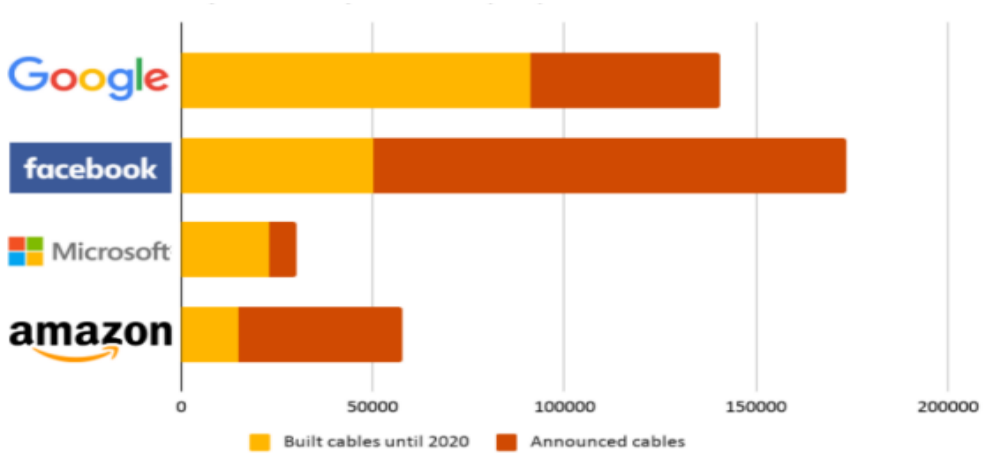


Figura 13: PWC, Study to Monitor Connectivity – Connecting the Eu to its partners through submarine cables, European Commission, 2022.

L'ingresso in questo mercato non si deve tanto al fatto che gli investimenti in cavi sottomarini siano ritenuti redditizi per queste aziende bensì al valore strategico che possiedono per le principali attività degli OTT. Infatti, essi necessitano di una larghezza di banda in continuo aumento che supporti il sempre maggiore utilizzo del cloud da parte della società. Per questo motivo, queste aziende non sono solo i principali proprietari di cavi sottomarini ma sono anche i soggetti che maggiormente li utilizzano, come dimostrato dal grafico in figura 15.

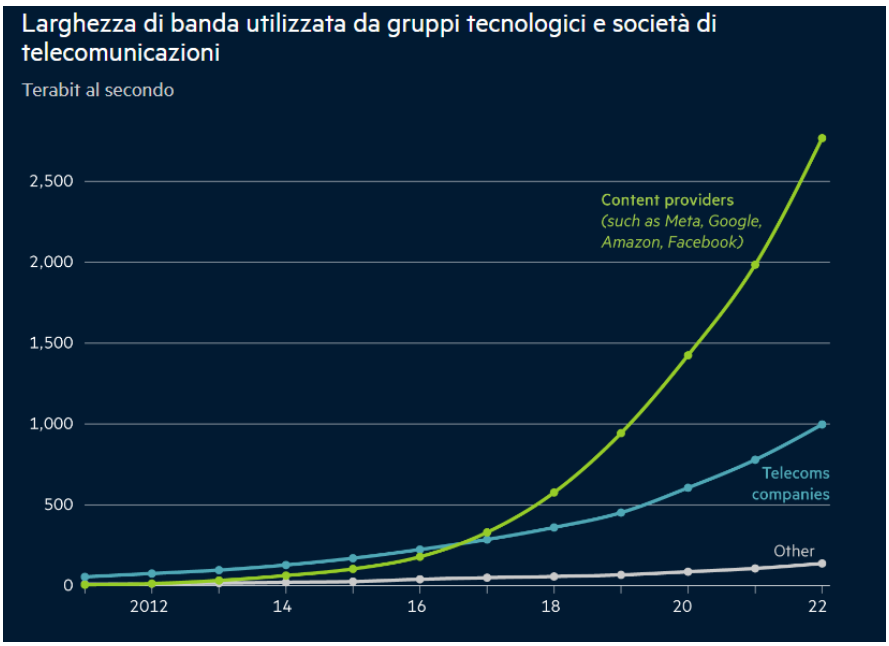


Figura 14: Anna Gross, Alexandra Heal, Chris Campbell et al. "How the US is pushing China out of the internet's plumbing", Financial Times, 13 giugno 2023. Accessibile a https://ig.ft.com/subsea-cables/.

Le incertezze sullo sviluppo del mercato sono molte a partire dal ruolo che avranno Amazon e Microsoft nei prossimi anni a livello di investimento, se vi sarà l'entrata nel mercato di nuovo Content Providers (Zoom, Dropbox, Apple) e se questi attori decideranno di rivendere parte della loro capacità di trasmissione all'ingrosso o di utilizzarla soltanto per sé.

2.6 ORGANIZZAZIONI INTERNAZIONALI E UNIONE EUROPEA: LA GOVERNANCE GLOBALE DEI CAVI SOTTOMARINI

L'ultimo paragrafo del capitolo è dedicato alla governance che gestisce i cavi sottomarini. Questa sezione aiuterà a capire meglio le dinamiche geopolitiche che riguardano i cavi, perché i privati hanno un ruolo anche più importante degli stati e quale sia l'approccio ideato dall'Unione Europea in termini di governance. Difatti, uno dei punti cruciali della ricerca risiede nel rapporto tra il campo della sicurezza nazionale, di cui gli stati membri sono particolarmente gelosi, e quello delle infrastrutture strategiche da cui tutti i paesi europei dipendono e che per questo motivo sono regolate anche da Bruxelles. I cavi sottomarini si contraddistinguono per essere una materia ibrida caratterizzata dalla presenza di più attori, più legislazioni e più interessi in gioco. Questa pluralità si riversa nella governance che risulta essere spezzettata tra più enti e più livelli. In via generale, è possibile affermare che vi è un livello internazionale composto dai trattati internazionali quali l'UNCLOS e dalle organizzazioni internazionali e relative autorità, un ambito regionale composto da ulteriori organizzazioni di carattere sovranazionale come l'Unione Europea e infine la legislazione nazionale. La complessità di cui sopra, è data soprattutto dalla presenza di ulteriori soggetti regolatori non istituzionali che però ricoprono un ruolo significativo come nel caso dell'ICPC o dei comitati regionali come l'Associazione nordamericana dei cavi sottomarini (NASCA). L'importanza di quest'ultimi soggetti è dovuta proprio all'assenza di enti regolatori unici o di agenzie specifiche sui cavi sottomarini che abbiano un'autorità chiara e ben disciplinata in materia.

2.6.1 Organizzazioni Internazionali

Come anticipato, nell'ambito dei cavi sottomarini è possibile parlare di "governance globale" per delineare la struttura giuridica che produce l'insieme di norme, vincolanti e non, del settore. Il giurista Armin Von Bogdany ha definito l'autorità pubblica come "l'assunzione e l'applicazione di decisioni unilaterali prese in nome e nell'interesse di un'entità generale"[189]. Tuttavia, l'autore aggiunge anche che "il concetto di governance globale riconosce l'importanza delle istituzioni internazionali ma sottolinea la rilevanza degli attori e degli strumenti di natura privata o ibrida"[190]. Nella pratica, gli

[189] A. Von Bogdany, M. Goldman, The Exercise of International Public Authority through National Policy Assessment, International Organizations Law Review, vol.5, pp. 241-298.
[190] Ibidem.

attori non statali sono in grado di definire standard non vincolanti ma a cui tutti gli operatori del settore reputano vantaggioso attenersi[191]. Questa dinamica è stata possibile in quanto nessuna organizzazione internazionale ha assunto il ruolo di agenzia leader per quanto riguarda le questioni legali, tecniche e consultive nell'ambito dei cavi sottomarini. Il diritto del mare e quello delle telecomunicazioni rappresentano la branca giuridica maggiormente competente e per questo motivo le principali agenzie internazionali che si occupano dei cavi sono l'UIT (Unione Internazionale delle Telecomunicazioni) e l'IMO (Organizzazione Marittima Internazionale). Inoltre, hanno un ruolo rilevante anche le istituzioni create dalle UN per dare applicazione all'UNCLOS: la Commissione sui Limiti della Piattaforma Continentale e l'Autorità Internazionale dei Fondali Marini. L'UIT ha il compito di sviluppare standard tecnici per le tecnologie che operano nell'ambito dell'informazione e comunicazione in modo da facilitarne l'accesso nel mondo. A differenza delle altre agenzie delle Nazioni Unite, l'UIT è partecipata non solo da 193 paesi ma anche da istituzioni accademiche e circa 700 aziende. Per quanto riguarda i cavi, l'agenzia si occupa principalmente delle trasmissioni che vi passano all'interno e non della sua infrastruttura. L'IMO si occupa di fornire regolamenti e standard, concordati su base internazionale, per la sicurezza, la protezione e le prestazioni ambientali del trasporto marittimo. Funziona come un forum i cui partecipanti sono gli stati, la società civile l'industria del trasporto marittimo. L'IMO si occupa dei cavi occasionalmente e solo per quanto riguarda le navi specializzate nel cablaggio e nelle riparazioni. La CLCS si occupa di definire i limiti territoriali della piattaforma continentale oltre le 200 miglia secondo le previsioni stabilite dall'UNCLOS. Sebbene i cavi sottomarini rientrino nella giurisdizione dell'UNCLOS, la Commissione non li affronta in quanto non influiscono sui confini della piattaforma. L'ISA è l'organizzazione attraverso la quale gli stati dovrebbero organizzare e controllare le attività che si svolgono sui fondali. Anche in questo caso, i cavi sottomarini non sono l'oggetto di analisi e regolamentazione principale ma l'agenzia ha redatto alcuni documenti in collaborazione con il Comitato Internazionale per la Protezione dei Cavi.

2.6.2 Il Comitato Internazionale per la Protezione dei Cavi Sottomarini

L'ICPC è stato fondato nel 1958 sotto il nome di Cable Damage Committee. Attualmente è un'associazione privata gestita dalla ICPC Ltd che è una società senza scopo di lucro con sede nel Regno Unito. Ad oggi conta oltre 200 membri provenienti da 70 diversi paesi[192]. Il suo scopro principale è quello di proteggere i cavi sottomarini dalle attività umane e dai disastri naturali tramite la creazione di standard e precauzioni internazionalmente riconosciuti. Le sue decisioni non sono

[191] Daria Shvets, The International Legal Regime of Submarine Cables: a Global Public Interest Regime, Universitat Pompeu Fabra Barcelona, 2020, pp.81.
[192] Sito web dell'ICPC, sezione "About the ICPC", Accessibile a https://www.iscpc.org/about-the-icpc/.

vincolanti e non si occupano di casi locali. Inoltre, è bene specificare come sia vietato parlare di costi e dinamiche di mercato all'interno di questo forum. Il comitato è il principale ente di regolamentazione per i cavi sottomarini e vanta uno status internazionale non indifferente. L'ICPC è l'esempio di come un attore privato non statale possa ricoprire un ruolo di interesse pubblico proprio come descritto dal concetto di governance globale. L'importanza di questo ente si spiega con l'assenza di attori istituzionali che sappiano ricoprire tale funzione e con l'esigenza da parte dei privati di regolare il proprio settore. Nonostante la funzione di interesse pubblico ricoperta, l'ICPC non è assimilabile al concetto di "organizzazione internazionale"[193] in quanto l'ICPC non è stata fondata tramite un trattato internazionale ratificato dagli stati ma come un'entità giuridica privata e non ha a sua volta la capacità di concludere trattati internazionali. Il suo status di organizzazione internazionale *de facto* è dimostrato dalla capacità dei suoi organi di prendere decisioni indipendenti rispetto ai suoi membri, di funzionare tramite l'affiliazione di stati ed enti privati[194] ed infine dalle collaborazioni con organizzazioni internazionali ufficiali come l'UNEP, l'ISA e l'ITU.

2.6.3 UNIONE EUROPEA

All'interno dell'Unione Europea si presentano le stesse problematiche di governance viste nel paragrafo precedente: tanti enti e modelli diversi che portano alla mancanza di una visione multidisciplinare del settore con chiare difficoltà di coordinamento e di chiarezza in quali siano i centri decisionali. In questo paragrafo non si intende analizzare la strategia europea e le politiche pubbliche che ne sono conseguite in questi anni nella protezione delle infrastrutture critiche (il tema sarà approfondito nel capitolo 4) ma si vuole esclusivamente dare un quadro generale della governance dei paesi membri e dell'UE per quanto concerne i cavi sottomarini.

L'infrastruttura dei cavi sottomarini sta guadagnando sempre maggiore rilevanza negli interessi strategici europei ma al momento ancora non è stata elaborata una struttura e una strategia inerente esclusivamente a questo ambito. Per questo motivo, il tema è oggetto di attenzione da parte di cinque diversi campi di intervento dell'Unione Europea: in via principale dalle politiche di sicurezza marittima e cibernetica, in via secondaria dalla governance degli oceani e dalle politiche infrastrutturali e digitali. Infine, l'azione esterna che compie l'Unione Europea a livello diplomatico

[193] "Si intende un'organizzazione istituita da un trattato o da un altro strumento di diritto internazionale e dotata di personalità giuridica internazionale propria. Le organizzazioni internazionali possono includere come membri, oltre agli Stati, altri enti". Vd. Op. Cit, Daria Shvets, The International Legal Regime of Submarine Cables: a Global Public Interest Regime, 2020 .

[194] Tali soggetti devono fare richiesta ed essere accettati solo se dimostrano di avere un comprovato interesse a far parte del comitato e, in seguito, devono pagare una quota di iscrizione di 2500£. Vd. Il sito web dell'ICPC, sezione "About Us", Accessibile a https://www.iscpc.org/about-the-icpc/ .

e militare tiene fortemente conto dei cavi sottomarini, specialmente dall'inizio del conflitto Russo-Ucraino.

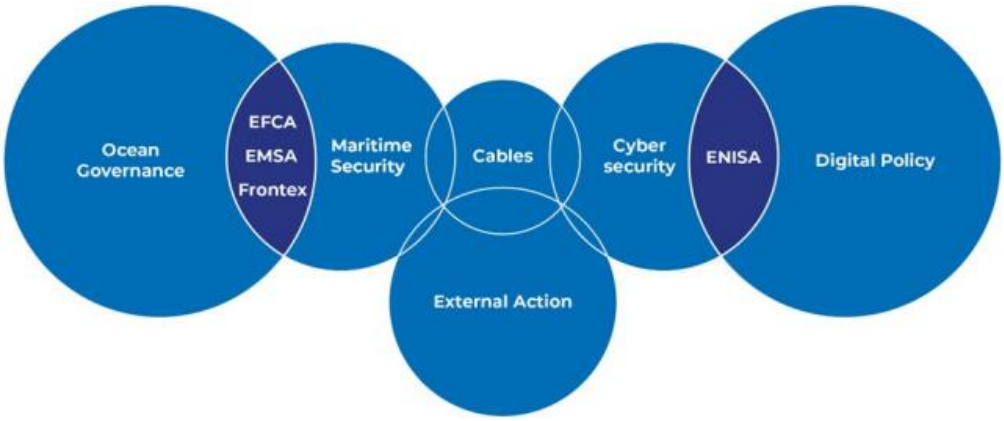


Figura 15: C. Bueger et al., Security Threats to Undersea Communications Cables and Infrastructure: Consequences for the EU, Sottocommissione del Parlamento Europeo per la Sicurezza e Difesa, p.40.

2.6.4. Sicurezza Marittima e Cyber Security

La sicurezza marittima è sempre stato un tema di grande attenzione da parte di Bruxelles ma il focus era soprattutto sui crimini marittimi come la pirateria, il traffico di esseri umani e la gestione delle rotte clandestine di immigrazione. Un approccio maggiormente olistico è stato sancito dalla "Strategia per la Sicurezza Marittima dell'Unione Europea" (EUMSS)[195] che ha posto la protezione dei cavi sottomarini come un tema dell'agenda dell'Unione Europea. Successivamente, il piano d'azione dell'EUMSS del 2018 ha enfatizzato il ruolo dell'EMSA, Frontex e dell'EFCA nella sorveglianza e protezione delle infrastrutture critiche marittime e la loro importanza. Tuttavia, nel report del 2020 con cui si analizzava lo stato di implementazione di queste misure non vi sono particolari riferimenti a questo settore. Tra le agenzie di sicurezza marittima più rilevanti nel campo dei cavi sottomarini vi sono l'EFCA, l'EMSA e Frontex. L'EFCA è l'ente regolatore della pesca in ambito europeo e ha voce in capitolo proprio perché l'attività ittica è tra le principali cause di danneggiamento dei cavi. L'EMSA è invece l'ente incaricato della protezione marittima ed in special modo del controllo della navigazione tramite l'Automated Identification System (AIS) che è il GPS delle imbarcazioni navali o tramite le immagini satellitari con il progetto Copernicus. Sebbene l'EFCA disponga dei mezzi per le attività di sorveglianza sulle acque europee, al momento non possiede alcun mandato specifico relativo alla protezione dei cavi sottomarini[196]. Infine vi è Frontex, il cui scopo principale è la prevenzione dell'immigrazione clandestina e più in generale del controllo delle frontiere marittime

[195] Consiglio dell'Unione Europea, Strategia per la Sicurezza Marittima dell'Unione Europea, 11205/14, 24 Giugno 2014. Accessibile a https://data.consilium.europa.eu/doc/document/ST%2011205%202014%20INIT/EN/pdf.
[196] C. Bueger et al., Security Threats to Undersea Communications Cables and Infrastructure: Consequences for the EU, Sottocommissione del Parlamento Europeo per la Sicurezza e Difesa, 2022.

tramite il supporto dei singoli stati membri e dell'EMSA. Ad oggi i cavi in fibra ottica non sono oggetto della sua azione di controllo.

Negli ultimi anni la cyber sicurezza ha assunto un ruolo primario tra le politiche europee di sicurezza. Anche se oggi può apparire come un qualcosa di scontato, bisogna ricordarsi come si trattasse di un campo a lungo ricompreso nel novero della sicurezza nazionale e quindi di completa competenza statale. Solo nel 2013 si è assistito al primo cambio di passo con la prima strategia in ambito cyber di carattere europeo[197] e poi con la prima direttiva NIS del 2016 (N.1148)[198] con cui venne approvato il GDPR e sancita la necessità di una collaborazione tra pubblico e privato nel settore. Direttiva che trovò la sua applicazione nel Regolamento 452 del 2019. Nel 2017 il pacchetto di sicurezza cibernetica europeo è stato aggiornato introducendo importanti rafforzamenti all'ENISA e l'elaborazione del Blue Print ossia il meccanismo che si attiva a livello europeo qualora uno stato membro subisca violazioni cibernetiche su larga scala che possono avere conseguenze transfrontaliere. Infine, tramite gli ultimi provvedimenti europei[199] si è cercato di uniformare il framework legislativo degli stati membri e di estendere la lista di infrastrutture critiche europee che devono essere oggetto della massima protezione da parte degli stati membri, tra cui rientrano i cavi sottomarini[200]. Come nel caso delle agenzie di sicurezza marittima, l'ENISA non ha redatto un piano strategico per la protezione dei cavi sottomarini ma esclusivamente un report contenente delle "buone pratiche" che gli stati membri dovrebbero seguire[201]. Il meccanismo congiunto della Direttiva CER e NIS2 sembra essere la giusta strada nell'indirizzare i paesi verso una maggiore uniformità legislativa e una condivisione delle informazioni ma nella pratica i cavi sottomarini non sono ancora stati direttamente coinvolti da questi meccanismi ed è quindi difficile giudicarne l'effetto.

2.6.5 Gli altri campi di intervento: governance marittima, politica digitale e infrastrutture, politica estera.

Il percorso di digitalizzazione dell'Unione Europeo è iniziato in leggero anticipo rispetto a quello della cyber sicurezza ma, come espresso da Ursula von der Leyen, si tratta di due facce della stessa

[197] European Commission, 'Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN(2013), 7 Febraio 2013.
[198] Gazzetta Ufficiale dell'Unione Europea, "Direttiva (UE) 2016/1148 del Parlamento Europeo e del Consiglio del 6 Luglio 2016 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione", https://eur-lex.europa.eu/eli/dir/2016/1148/oj/ita/pdf .
[199] Gli atti a cui si fa riferimento sono le Direttive UE 2022/2555, 2022/2256, 2022/2257 ed il Regolamento 2022/2254. Accessibile a https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=OJ:L:2022:333:FULL&from=IT
[200] La Direttiva NIS2, Art.7, comma d, richiede che gli Stati Membri adottino politiche "relativi al mantenimento della disponibilità generale, dell'integrità e della riservatezza del nucleo pubblico dell'open internet, compresa, se del caso, la sicurezza informatica dei cavi di comunicazione sottomarini;
[201] Georgia Bafoutsou, Maria Papaphilippou, Marnix Dekker, Subsea Cables – What is at Stake?, ENISA, Luglio 2023.

medaglia[202]. La strategia europea si concentra sulla sovranità digitale e quindi il controllo e protezione dei dati dei cittadini europei. E' in questo concetto che si inseriscono il "Digital Markets Act"[203], il "Digital Services Act"[204] e soprattutto l'European Data Gateway Platforms Strategy[205]. Tuttavia, anche in questo settore non si registra una particolare attenzione ai cavi sottomarini e specialmente al grado di dipendenza dell'Europa da infrastrutture costruite da soggetti legati a paesi stranieri come la Cina. Il tema dei cavi sottomarini è cruciale per l'Europa sia da un punto di vista di protezione da possibili attacchi che come strumento di diplomazia e cooperazione internazionale. In questo senso, l'UE gioca un ruolo cruciale nello sviluppo della connettività dell'Africa e dei collegamenti anche con il Sud America. Una strategia incentrata sulla sicurezza delle comunicazioni internazionali sarebbe pienamente coerente con la visione europea di digitalizzazione e cyber sicurezza degli ultimi anni che ha visto il continente affermarsi come principale protettore dei dati dei cittadini nei confronti degli stati o delle aziende. Tuttavia, nonostante la presenza di numerosi progetti europei inerenti il digitale, le infrastrutture critiche ed il dominio subacqueo, ancora non si è dato un particolare risalto a questo tema.

2.6.6 Stati Membri

I diversi approcci assunti dagli stati membri dipendono in gran parte dalla rilevanza strategica che hanno i cavi sottomarini per i relativi governi. In tal senso, è possibile affermare che gli stati maggiormente attenti alla tematica sono quelli che sono stati esposti all'attività marittima ostile della Russia come il Portogallo[206] e la Francia e ciò è dimostrato dai numerosi documenti pubblicati da questi stati sul tema[207]. I paesi del Mediterraneo come Spagna e Italia mostrano un ristretto interesse sui cavi sottomarini in quanto la loro attenzione è maggiormente dirottato sull'immigrazione clandestina. In questi paesi il tema è trattato principalmente nei documenti strategici delle relative marine[208]. Chiaramente gli stati insulari che dipendono esclusivamente dai cavi sottomarini per le loro telecomunicazioni sono quelli maggiormente preoccupati dalla tematica come nel caso di Irlanda,

---

[202] U. Von der Leyen, 'A Union that Strives for more. My agenda for Europe', European Commission, 2019, p.13.
[203] Commissione Europea, Proposta di REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO relativo a mercati equi e contendibili nel settore digitale, COM(2020) 842 final, 15 dicembre 2020.
[204] Commissione Europea, Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services, Official Journal of the European Unioni, 19 ottobre 2022.
[205] Digital day 2021: Europe to reinforce internet conncectivity with global partners, Accessibile a https://digital-strategy.ec.europa.eu/en/node/9588/printable/pdf#:~:text=In%20the%20'Data%20Gateways'%20declaration,into%20account%20the%20international%20strategy.
[206] Sotto la sua presidenza al Consiglio Europeo è stata approvata la "European Data-Gateway Platforms Strategy" che rappresenta il documento strategico europeo in ambito informatico e digitale.
[207]Ministero della Difesa Francese, Seabed Warfare Strategy, 2022. https://www.archives.defense.gouv.fr/content/download/636001/10511909/file/20220214_FRENCH%20SEABED%20STRATEGY.pdf. Vedi anche . J. Pousson, 'Guerre en Ukraine : la Russie peut-elle vraiment couper Internet en Europe?', Le Parisien, 4 March 2022.
[208] Stato Maggiore della Marina, Marina Militare Linee di Indirizzo Strategico, Rivista Marittima, 2019.

Regno Unito e Malta. Infine, bisogna sottolineare come anche la governance marittima stabilita incida sulle modalità con cui si trattano i cavi sottomarini.

In questi paesi è possibile individuare tre diversi modelli di governance. Il primo, assegna la leadership ai soggetti incaricati della sicurezza nazionale e della marina. In Francia, il Segretariato Generale per la Difesa e la Sicurezza Nazionale, organo interministeriale sotto il Primo Ministro francese, svolge un ruolo importante nel garantire e coordinare le prospettive di sicurezza nazionale del settore sottomarino, mentre il Secretariat Général à la Mer (SGMer) ha il compito di coordinare i compiti amministrativi relativi alla protezione dei dati che passano nei cavi. Inoltre, la Marina Francese ricopre un ruolo fondamentale nella protezione dei cavi in collaborazione con le società private[209]. A queste si devono aggiungere le agenzie che a diverso titolo si occupano della sicurezza interna ed esterna del paese come L'Agence Nationale dè la sècuritè des systèmes d'information. Il secondo modello presenta un approccio completamente opposto ed è quello della Danimarca dove la sorveglianza e protezione dei cavi sono lasciate alle compagnie private mentre la Guardia Costiera e l'Autorità Marittima Danese si occupano esclusivamente di stabilire quali siano le zone protette per i cavi e di assegnare i permessi di installazione. Non è un caso che la massima autorità in ambito di cavi sottomarini sia il Danish Cable Protection Committee (DKCPC) che possiede la medesima struttura e scopi dell'ICPC[210]. Infine, vi è un terzo modello che rappresenta una via di mezzo tra i primi due proposti ed è quello di Malta in cui la leadership è assegnata dall'apposito Critical Infrastructure Protection Directorate (CIPD) che si trova sotto il Ministero degli Affari Interni e la Sicurezza Nazionale. La sua peculiarità è rappresentata dall'essere un centro unico di comando e sorveglianza per la sicurezza marittima ed informatica che collabora principalmente con le aziende private, tramite il potere di visita e ispezione ai landing sites, ma anche con le altre autorità civili (come la Malta Communication Authority) e la Marina. Sebbene questo approccio sembri essere il più razionale ed efficiente nell'affrontare la resilienza e la regolamentazione di questo settore, permangono dubbi circa la sua applicazione in paesi più grandi e con un numero di cavi sottomarini ben maggiori da controllare. Aldilà del modello preso in esame, in tutta Europa si riscontra una crescita nell'attenzione dei policymakers sul tema, in parte dovuto ai rischi concreti che il rinnovato espansionismo subacqueo russo ha messo in atto. Tuttavia, la criticità fondamentale che è relativa alla frammentazione del sistema di controllo in numerosissime agenzie, permane nella maggioranza dei paesi. Questo ha importanti conseguenze anche sul piano europeo dal momento che l'Europa funge

[209] Op.Cit,Daria Shvets, The International Legal Regime of Submarine Cables, 2020, pp.81., pp.38.
[210] Sito web del DKCPC, Sezione "Introduction to DKPCPC", Accessibile a https://dkcpc.dk/introduction-to-dkcpc/

da connettore ma per operare efficientemente deve ricevere le informazioni in modo chiaro, immediato e univoco mentre questo tipo di governance rende il processo più complicato.

CAPITOLO 3

3.0 I RISCHI E LA PROTEZIONE DEI CAVI SOTTOMARINI

Dopo aver analizzato il funzionamento dei cavi sottomarini, le implicazioni legali ed il comportamento dei privati nel settore, è possibile passare alla disamina delle minacce che lo riguardano. Come è stato evidenziato da Bueger e Liebetrau, sebbene i cavi sottomarini raccolgano un interesse sempre maggiore tra i ricercatori, la tematica viene concepita in "termini ristretti ed eccessivamente tecnici, senza che venga prestata piena attenzione alle questioni politiche più ampie che la rete solleva"[211]. Per questo motivo, i capitoli successivi hanno lo scopo di inquadrare questa tematica all'interno del dibattito internazionale sulla sicurezza identificando una serie di traiettorie di ricerca che espandono la portata teorica ed empirica della sicurezza dei cavi dati sottomarini.

Come tutte le infrastrutture critiche, i cavi sottomarini rappresentano un obiettivo sensibile per chiunque voglia arrecare un danno ad uno stato. Tuttavia, a differenza di altre infrastrutture, i cavi sottomarini possono anche essere utilizzati come vettori per attacchi digitali. Utilizzando il paragone citato nel primo capitolo, si potrebbe dire che i cavi possono essere infettati come succede con le vene. Una volta che un virus entra in circolo nel sangue, è molto più difficile circoscrivere il danno e lo stesso succede con i cavi sottomarini. Ad esempio, il sabotaggio di una landing station che si trova a Singapore potrebbe compromettere il sistema sanitario della California che si poggia proprio su quel cavo sottomarino per elaborare i dati dei suoi pazienti.

I cavi sottomarini si distinguono come il mezzo più rapido, economico e affidabile per la trasmissione globale dei dati. In un'era in cui la dipendenza del mondo dalla tecnologia digitale comprende comunicazioni civili, commercio, agricoltura, sanità, logistica militare e transazioni finanziarie, questi cavi subacquei racchiusi in acciaio e plastica sono diventati indispensabili per la sicurezza nazionale. Qualsiasi interruzione di questi cavi potrebbe paralizzare la regione colpita e spingere il mondo sull'orlo di una "nuova grande depressione"[212].

---

[211] Christian Bueger & Tobias Liebetrau, Protezione delle infrastrutture nascoste: la politica di sicurezza della rete globale di cavi dati sottomarini, Contemporary Security Policy, 42:3, 391-413, 2021.
[212] James Rickards, *The New Great Depression: Winners and Losers in a Post-Pandemic World* (New York: Portfolio/Penguin, 2021).

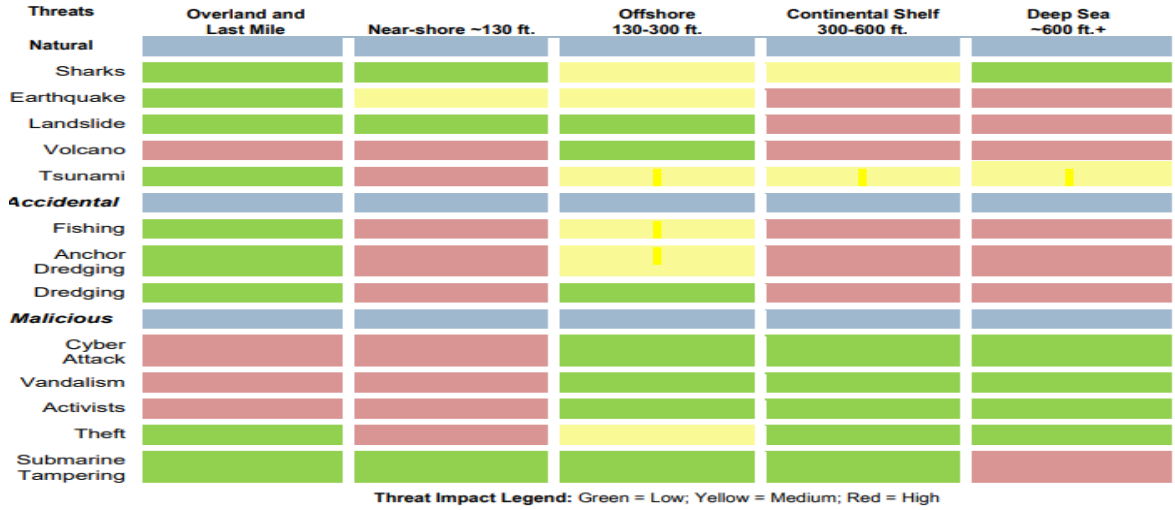


Figura 16: Figura 1: Fonte: Adattata da The Public-Private Analytic Exchange Program (AEP), the Department of Homeland Security's Office of Intelligence and Analysis (DHS/I&A)

Sebbene i cavi operino ad una sicurezza del 99.999% (5-9s)[213], rimane un'infrastruttura con delle forti fragilità rispetto ad attacchi esterni. Innanzitutto, i cavi sono grandi quanto un cavo da giardino, le loro rotte sono spesso lunghe migliaia di chilometri e questo ne rende impossibile una protezione fisica costante. Si aggiunga, che tali cavi non sono di proprietà degli stati e quindi anche la loro protezione è affidata in gran parte ai privati. Questo è solo uno dei paradossi che sono stati sottolineati in questo elaborato: gli Stati dipendono da strutture su cui hanno un potere limitato sia in termini decisionali che di sicurezza del sistema.

In questo capitolo si intende condurre un'attenta analisi delle minacce che consenta di individuare in maniera semplice e chiara chi sono gli attori che mettono a rischio il sistema e come si potrebbe intervenire per mitigare questi rischi. Per tale ragione, si metterà l'accento sulla differenza tra i danni accidentali, quello non accidentali e quelli legati al funzionamento stesso del sistema dei cavi sottomarini.

[213] Meglio noto come lo "standard dei cinque 9" che è solitamente utilizzato per infrastrutture come le centrali nucleari. Significa che dal punto di vista tecnico si tratta di un'infrastruttura che funziona il 99.999% del tempo. Vedi Op.Cit. Sechrist, New Threats, Old Technology - Vulnerabilities in Undersea Communications Cable Network Management Systems, pp.9.

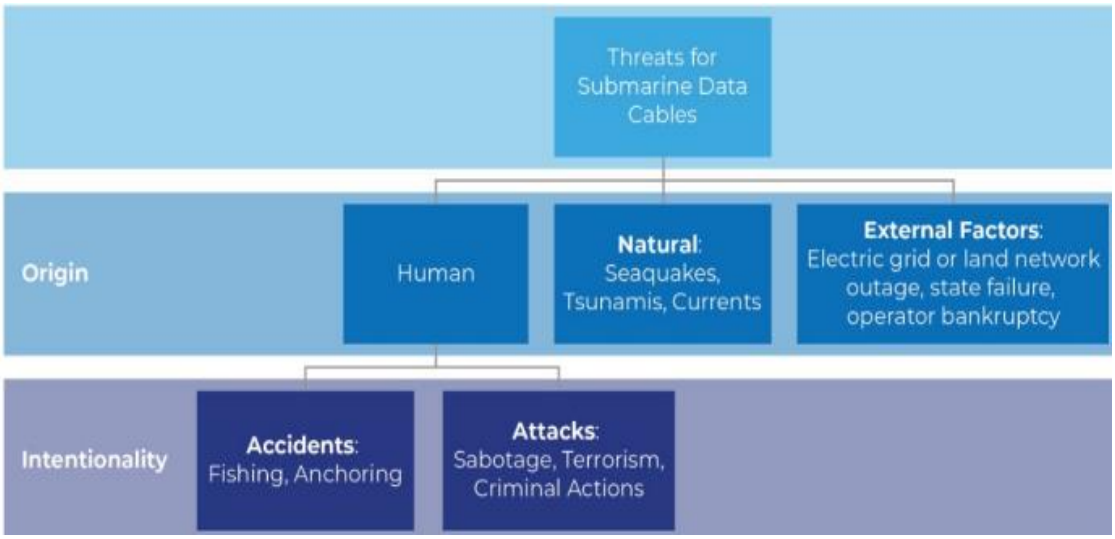


Figura 17: Bueger, Liebetrau, Security threats to undersea communications cables and infrastructure – consequences for the EU, giugno 2022.

3.1 DANNI ACCIDENTALI

I danni accidentali rappresentano la minaccia più frequente per i cavi sottomarini. Le Nazioni Unite stimano che, in media, vi siano tra i 150 e 200 cavi distrutti all'anno per cause legate ai fenomeni naturali e alla pesca[214]. Si tratta di una minaccia che non colpisce in egual modo tutti gli Stati in quanto quelli maggiormente sviluppati possiedono un livello di ridondanza del sistema abbastanza alto da poter sopportare il danneggiamento di qualche cavo mentre per i paesi in via di sviluppo la situazione è ben diversa. Ad esempio, l'Inghilterra è collegata all'Europa e agli Stati Uniti da oltre 30 cavi sottomarini a differenza di paesi come la Somalia che possiede solo due punti di approdo. Non è un caso che proprio in Somalia si è assistito ad uno dei casi più eclatanti degli ultimi anni quando nel 2017 metà del paese è rimasto senza internet con ricadute gigantesche per i milioni di cittadini non hanno potuto accedere alle cure mediche perché i loro documenti online erano irraggiungibili[215]. Si stima che la Somalia abbia sofferto perdite per un valore pari a 10 milioni di euro al giorno[216].

[214] C. Kavanagh. Wading Murky Waters: Subsea Communications Cables and Responsible State Behaviour, UNIDIR, Geneva, Svizzera, 2023.
[215] The Guardian, Somalia back online after entire country cut from internet for three weeks, Luglio 2017, Accessibile a https://www.theguardian.com/world/2017/jul/18/somalia-cut-off-from-internet-entire-country-three-weeks.
[216] Op. Cit. R. Sunak, Undersea Cables – Indispensable, Insecure, Policy Exchange.

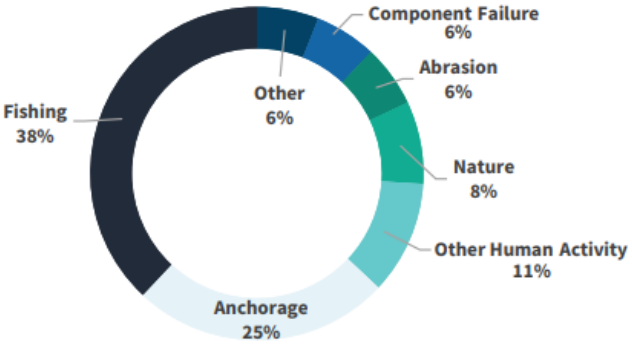


Figura 18: Alan Mauldin, "Cable Breakage: When and How Cables Go Down," TeleGeography, May 3, 2017, https://blog.telegeography.com/

3.1.1 Danni naturali

I fenomeni naturali rappresentano una minaccia considerevole per i cavi sottomarini in quanto le politiche di mitigazione del rischio sono di difficile applicazione e hanno effetti minori rispetto ai danni causati direttamente dall'uomo. Quando si parla di fenomeni naturali ci si riferisce in primis all'impatto che può avere l'acqua sull'infrastruttura. Gli tsunami e le forti correnti che si creano in alcune zone del mondo hanno la capacità di spostare i cavi sottomarini da dove sono posati, specialmente quando questi non sono posizionati sottoterra ma solo appoggiati sul fondale marino.

I terremoti sono tra i fenomeni con il maggiore impatto sui cavi sottomarini per via della loro potenza. Ad esempio, il terremoto che ha colpito il Giappone nel 2011 ha distrutto 4 dei 20 cavi di cui disponeva il paese. Se nel caso del Giappone è stato possibile reindirizzare senza troppi rallentamenti il traffico di rete su altri cavi, lo stesso non è stato fatto nel caso del terremoto di Luzan dove oltre il 40% della flotta mondiale di navi per la riparazione dei cavi ha impiegato sette settimane per completare il lavoro di riparazione e l'interruzione di Internet era ancora in corso due mesi dopo il terremoto iniziale[217].

Il rischio che un cavo sia danneggiato per eventi naturali dipende fortemente dall'area geografica in cui è installato il cavo ed è uno dei motivi per cui le aziende spendono moltissimo tempo nel mappare i fondali e studiare il comportamento del mare prima di procedere con la posa del cavo. Si tratta di una tipologia di minaccia di media frequenza[218] ma con un impatto molto alto sull'infrastruttura[219].

[217] Ivi, pp. 39.
[218] Solamente nel periodo tra il 2006 ed il 2012 sono stati registrati tre importanti terremoti che hanno causato la rottura di più cavi sottomarini. Secondo alcuni studi, un terremoto di magnitudo 6.0 è in grado di mettere in serio pericolo qualsiasi cavo sottomarino. Per tali ragioni, i fenomeni naturali non sono frequenti ma neanche rari. Si veda Liu Aiwen, "Response analysis of a submarine cable under fault movement," Earthquake Engineering and Engineering Vibrationm Marzo 2009.
[219] Op.Cit M. Sechrist, New Threats, Old Vulnerabilities, 2013.

Tali avvenimenti sono più devastanti nelle aree dove vi sono dei "colli di bottiglia" per i cavi sottomarini come lo stretto di Gibilterra o di Malacca. Ad esempio, oltre il 40% delle interruzioni di servizio dei cavi sottomarini tra il 2004 e il 2009 si sono verificate nella regione del Pacifico settentrionale (in prossimità dello stretto di Luzon, al largo delle coste di Taiwan), a causa di terremoti e altre cause naturali. Nella regione dell'Atlantico settentrionale, invece, i terremoti non sono una delle principali preoccupazioni. Per l'Italia e l'Europa nel suo complesso, le principali rotte dei cavi in fibra sono lo Stretto di Gibilterra per il quale passano almeno 7 cavi sottomarini ed il Canale di Suez dove ne passano almeno 16 di cavi.

Le risposte degli oceani ai cambiamenti climatici attuali e previsti hanno il potenziale per influire sulla rete di cavi sottomarini attraverso l'intensificazione dei pericoli naturali legati all'innalzamento del livello del mare, ai cambiamenti nella frequenza e nell'intensità delle tempeste, che influenzeranno gli effetti delle onde e delle correnti sui cavi e agli eventi di pioggia che possono aumentare le inondazioni fino formare correnti di torbidità potenzialmente in grado di danneggiare i cavi. Per questo motivo, dopo i terremoti di magnitudo 7.0 e 9.0 avvenuti rispettivamente nel 2006 e nel 2011 sulle coste di Taiwan e del Giappone, il consorzio Southeast Asia-Japan ha annunciato la costruzione di un nuovo cavo, ad opera di TE SubCom e NEC Corporation, con lo scopo di avere delle linee di comunicazione alternative in caso di terremoti in quell'area. Sebbene il percorso del cavo Asian Submarine-cable Express (ASE) non sia il più breve per unire la terraferma con il Giappone, rappresenta sicuramente una via più sicura che consente di evitare rallentamenti o la distruzione del cavo[220].

3.1.2 Danni fisici

Le minacce fisiche sono quelle situazioni in cui un attore può manipolare e/o provocare danni effettivi ai componenti fisici del cavo. Possono essere intenzionali o accidentali. Nel primo caso rientrano tutte le azioni di sabotaggio e spionaggio che mirano ad intercettare le informazioni che passano per i cavi. Nel secondo caso vi sono i fenomeni naturali o la rottura di cavi per colpa delle ancore durante la pesca (2/3 delle rotture)[221].

Ogni anno il numero di cavi danneggiati si aggira tra i 150 ed i 200[222]. Alcune tecniche di pesca come le reti a strascico e le draghe, sono particolarmente rischiose per i cavi, ma restano diffuse in alcune zone dell'Asia. Gli incidenti di ancoraggio si verificano spesso quando le ancore sono

[220] Valerie C. Coffey, Sea Challenge – The Challenges facing Submarine Optical Communications, Optic e Photonics News, Marzo 2014.
[221] Op.Cit. Securing Subsea Cable Critical Infrastructure, Seton Hall University, pp. 13-14.
[222] L. Carter et al., Submarine Cables and the Oceans - Connecting the World, UNEP-WCMC Biodiversity Series no. 31, Cambridge, UK , 2009, Accessibile a https://www.iscpc.org/ documents/?id=132.

inavvertitamente lasciate cadere e trascinate sul fondo del mare. Inoltre, Anche le condizioni meteorologiche estreme possono trascinare le imbarcazioni contro i cavi. L'ICPC (International Cable Protection Committee) ha sottolineato come si siano riscontrati molti casi nei quali i pescherecci hanno ostacolato l'attività delle navi per le riparazioni o di posa dei cavi.

3.2 DANNI INTENZIONALI

3.2.1 Analisi delle minacce provenienti da attori non statali

I cavi sottomarini sono un'infrastruttura particolarmente fragile se si considera che la loro dimensione è paragonabile a quella di un tubo da giardino. Per questo motivo, le aziende tendono a sotterrare i cavi invece che posarli semplicemente sul fondale marino in modo da tenerli maggiormente protetti dalle ancore e reti da pesca. Inoltre, nelle zone maggiormente a rischio i cavi vengono costruiti con dei rivestimenti ulteriori. Tuttavia, questi metodi sono utili per mitigare i rischi accidentali ma funzionano meno nell'affrontare degli attacchi volontari da parte dell'uomo. In questo paragrafo si analizzeranno brevemente alcune modalità di attacco utilizzate per danneggiare i cavi sottomarini in fibra ottica.

Innanzitutto, i pescherecci o le navi di ricerca possono essere convertiti allo scopo di distruggere i cavi sottomarini con l'ausilio dei cosiddetti "*improvised cutting devices*" (ICDs) come, ad esempio, delle normalissime ancore[223]. Si tratta di armi facili da costruire ed utilizzare. Inoltre, questi attacchi vengono lanciati da imbarcazioni civili che possono facilmente nascondersi nel traffico marittimo senza destare particolari sospetti.

Una seconda tipologia di minaccia è quella legata agli esplosivi sottomarini come le mine navali oppure gli ordigni esplosivi marittimi improvvisati (MIEDs) che possono essere azionati anche a distanza[224]. Si tratta di esplosivi facili da costruire e poco costosi. Vista la scarsa protezione dei cavi sottomarini, bastano piccole esplosioni per poter distruggere l'infrastruttura in questione. Per poter utilizzare queste armi sono necessarie delle competenze maggiori rispetto agli ICDs, in special modo per quanto riguarda le capacità di immersione.

La terza forma di attacco è rappresentata da natanti sommergibili o da droni e sottomarini di tipo militare con o senza equipaggio. Si tratta di un dispositivo d'arma che si sta sempre più diffondendo.

[223] C. Bueger, T. Liebetrau, J. Franken, Security threats to undersea communications cables and infrastructure – consequences for the EU, European Parliament's sub-committee on Security and Defence, pp. 29, 2022.
[224] Questi dispositivi sono tradizionalmente fatti in casa e sono progettati per provocare morte o lesioni utilizzando esplosivi da soli o in combinazione con sostanze chimiche tossiche, tossine biologiche o materiale radiologico. Vedi P. Paulo , Richard Jimenez, Bobby Rowden, Christopher Causee, Simulation Analysis of a System to Defeat Maritime Improvised Explosive Devices (MIED) in a US Port, International Institute of Strategic Studies, The Military Balance, 2017.

Difatti, l'ambiente sottomarino è particolarmente ostico per l'uomo ed è per questo che assumono importanza i veicoli comandati a distanza. Addirittura, anche le organizzazioni criminali stanno ricorrendo a questi strumenti[225]. In questo caso l'utilizzo che ne viene fatto è duplice: questi natanti sono utilizzati sia per operazioni di intelligence in quanto permettono di avvicinarsi ai cavi sottomarini senza essere notati e sono dotati di appositi bracci meccanici che permettono di interagire con il cavo per estrapolarne le informazioni ma possono anche essere utilizzati per operazioni di sabotaggio tramite l'installazione di mine o MIEDs[226]. A differenza delle precedenti armi, i sottomarini telecomandati sono molto più difficili da rintracciare ma richiedono costi e competenze notevolmente più alti[227].

Infine, gli attacchi fisici possono essere anche diretti all'infrastruttura a terra che gestisce i cavi sottomarini (*dry plant*). In questo scenario i danni che ne scaturirebbero sarebbero ancora maggiori in quanto verrebbe coinvolto un numero nettamente maggiore di cavi. Gli scenari possibili presentano diversi gradi di pericolosità e di probabilità che vengano messi in atto. Ad esempio, molto dipende se ci troviamo in uno scenario di guerra aperta come quello che si è presentato tra Russia ed Ucraina oppure di guerra ibrida. Nel primo caso è plausibile aspettarsi attacchi coordinati ai cavi, alle CLS e alle navi di riparazioni con ordigni di diverso tipo mentre in un contesto di conflitto a bassa intensità è più probabile aspettarsi attacchi isolati come quello al North Stream 2.

Per quanto concerne gli attori non statali che rappresentano una minaccia seria per il sistema dei cavi sottomarini, è interessante sottolineare due casi specifici come quello della pirateria ed il ruolo dello Yemen alla luce degli ultimi sviluppi geopolitici in questa regione[228]. Infatti, tra le minacce di natura antropica rientrano anche il furto di metalli preziosi come successo nel 2017 in Vietnam dove sono state arrestate 10 persone che avevano provato a tagliare dei cavi sottomarini per estrarne le materie prime di cui sono composti. Sebbene si sia trattato di un evento piuttosto eccezionale, l'industria è stata fortemente scossa da questa evenienza. La pirateria rappresenta un rischio non solo per i cavi anche per le navi che devono posarli. Non è un mistero che le navi commerciali rappresentino un bottino di eccezionale valore per questi attori.

[225] J. Guerrero, 'Narcosubmarines. Outlaw Innovation and Maritime Interdiction in the War on Drugs', Palgrave Macmillan, Singapore, 2020.
[226] C. Bueger, T. Liebetrau, J. Franken, Security threats to undersea communications cables and infrastructure – consequences for the EU, European Parliament's sub-committee on Security and Defence, pp. 29, 2022
[227] Ibidem.
[228] Gli USA hanno lanciato un'iniziativa multilaterale per contrastare gli attacchi del movimento yemenita contro navi commerciali: presente anche l'Italia e diversi paesi europei. Vedi "Una coalizione Anti-Houthi nel Mar Rosso", ISPI, 19 Dicembre 2023. Accessibile a https://www.ispionline.it/it/pubblicazione/una-coalizione-anti-houthi-nel-mar-rosso-157403

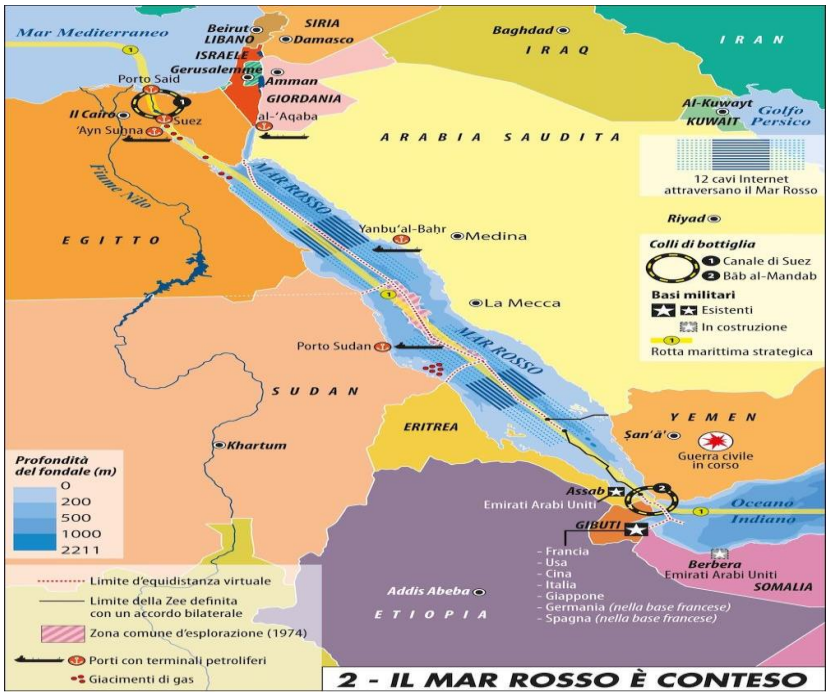


Figura 19: Mappa di Laura Canale, La vera posta in gioco nella guerra in Yemen è il bottino marittimo, Limes, 2020.

Come si può notare dalla Figura 3, lo Yemen possiede una posizione cruciale nella geografia mondiale dei cavi sottomarini in quanto lo stretto di Bab-El Mandeb rappresenta una via obbligatoria per i 12 cavi che passano per il canale di Suez. La guerra civile in Yemen vede la forza ribelle degli Houthi controllare diverse postazioni sulla costa del paese che gli permettono di pianificare attacchi ai mercantili e petroliere tramite droni marittimi. Le capacità militari degli Houthi sono una minaccia reale e non potenziale (come dimostrato dalla distruzione del porto yemenita di Mokha nel settembre 2021) di carattere globale e non solo regionale. D'altronde la scelta degli Stati Uniti di comporre una task force che intervenga in questa regione non è solo per difendere il commercio ma anche i dati che passano al di sotto di queste navi e che, se manomessi, possono rappresentare una minaccia ancora più seria per la sicurezza nazionale statunitense.

In definitiva, le minacce da parte di attori non statali devono essere trattate seriamente in quanto la fragilità dei cavi sottomarini li rende un bersaglio di facile distruzione. Il pericolo di attività di intelligence e manomissione dei dati è estremamente più basso in quanto richiede mezzi e conoscenze che tali gruppi armati non possiedono. L'interesse da parte di questi soggetti di attaccare i cavi è sicuramente più basso rispetto a quello che possono avere attori statali ma ciò non vuol dire che sia inesistente e trascurabile. Infatti, i cavi sono un bersaglio che possiede un alto rapporto tra danni provocabili e difficoltà nel colpirlo. Infine, non bisogna scordarsi che gli attori non statali sono spesso supportati da stati e possono muoversi per conto di quest'ultimi come nel caso degli Houthi nello Yemen.

3.2.2 Le minacce provenienti da attori statali: il caso della Russia e della Cina

3.2.2.1 LA RUSSIA

L'interesse russo sui cavi sottomarini è dimostrato da diversi documenti NATO[229]e del Regno Unito. È ormai noto che la Federazione Russa stia investendo notevoli risorse sulle sue forze subacquee in modo da poter avere una presenza silenziosa ma letale in diverse aree del globo. L'invasione dell'Ucraina ha reso ancora più evidente le capacità russe nella guerra asimmetrica di cui una parte rilevante è rappresentata dalla cyber-warfare. Il controllo delle informazioni è diventato sempre più cruciale ed è per questo che i cavi sottomarini rappresentano una potenziale miniera d'oro per quelli stati che intendono manipolare i dati.

La flotta navale russa è sempre stata una delle più grandi minacce per l'Occidente. Ciò era dovuto in gran parte alla disponibilità di un arsenale nucleare dispiegabile dai mari più remoti. Tuttavia, con la dissoluzione dell'Unione Sovietica le forze armate sono entrate in una spirale di declino e la ricerca e sviluppo in nuovi armamenti si è dovuta fermare per dirigere le risorse in altri settori. Questa tendenza si è invertita e dal 2010 in poi la spesa in armamenti militari in rapporto con il PIL è sempre aumentata[230]. I russi hanno dichiarato che intendono diventare la seconda flotta più imponente entro il 2027[231]. Flotta che comprende lo Yantar che sebbene sia classificata dai russi come una nave da ricerca è nota per trasportare droni subacquei[232] ed i mini-sottomarini AS-37 che possono raggiungere i 6000 metri di profondità e sono stati avvistati a largo della costa irlandese lungo la rotta dei cavi Norse e AE Connect-1 che uniscono Europa e USA[233]. A Sud-est dell'Irlanda, ai confini della sua ZEE, la Russia ha messo in atto diverse esercitazioni navali in prossimità di cavi che collegano l'Inghilterra, la Francia e gli Stati Uniti.

[229] N. Soames, 'Evolving Security in the North Atlantic', NATO Defence and Security Committee (DSC), Sub-Committee on Transatlantic Defence and Security Cooperation (DSCTC), 13 Ottobre 2019; R. Sunak, Undersea Cables Indispensable, insecure, Policy Exchange, 2017.

[231] Ibidem.

[232] Lukas Trakimavičius, The Hidden Threat to Baltic Undersea Power Cables, Nato Energy Security Centre of Excellence, at 3, Accessibile a https://www.enseccoe.org/data/public/uploads/2021/12/the-hidden-threat-to-baltic-undersea-powercables-final.pdf.

[233] Riechmann, Deb. 2018. "Could Enemies Target Undersea Cables That Link the World?" AP News, March 30, 2018, sec. Russia.

Year	Billion Roubles	% GDP
2016	3,972	4.64
2015	4,026	4.98
2014	3,222	4.13
2013	2,783	3.92
2012	2,505	3.74
2011	2,029	3.40
2010	1,760	3.54

Figura 20: 2 International Institute of Strategic Studies, The Military Balance, 2017.

Le azioni russe si inseriscono a pieno nel concetto di guerra ibrida[234]che si è diffuso nell'ultimo decennio e di cui il dominio cyber e marittimo rappresentano alcune tra le principali minacce. La pressione interna viene esercitata attraverso mezzi politici, informativi o economici per indebolire un altro Stato con il sostegno della minaccia della forza convenzionale. La Russia utilizza tale tecnica in modo da poter danneggiare uno stato estero senza che si attivi l'articolo 5 della Nato di difesa reciproca e poter così negare ogni responsabilità in questi attacchi. In questo modo Putin ha potuto negare che nel Donbass ucraino vi fossero truppe russe dal momento che non possedevano mostrine dell'esercito regolare e allo stesso modo gli attacchi alla fibra ottica non sembrano poter giustificare una risposta armata da parte del paese attaccato.

Secondo l'ODNI, la Russia "è particolarmente concentrata nel migliorare la propria capacità di colpire le infrastrutture critiche, compresi i cavi sottomarini e i sistemi di controllo industriale, negli Stati Uniti e nei paesi alleati, perché compromettere tali infrastrutture dimostra la sua capacità di danneggiare le infrastrutture durante una crisi."[235] Il Cremlino ha continuamente sottolineato l'importanza del controllo di Internet come risorsa geopolitica chiave. Nel 2014, durante l'annessione illegale della Crimea da parte della Russia, sono stati segnalati casi di "manomissione di cavi in fibra ottica, che hanno causato interruzioni del servizio telefonico locale e Sistemi Internet"[236]. Ciò è stato possibile tramite la conquista di Simferopol[237] dove si trovava l'unico Internet Exchange Point operativo[238]. Sebbene il caso della Crimea rappresenti un unicum vista la disposizione geografica del

[234] Strategia militare, caratterizzata da grande flessibilità, che unisce la guerra convenzionale, la guerra irregolare e la guerra fatta di azioni di attacco e sabotaggio cibernetico. Treccani, Neologismi, 2017. Accessibile a https://www.treccani.it/vocabolario/guerra-ibrida_%28Neologismi%29/
[235] Annual Threat Assessment of the U.S Intelligence Community, Office of the Director of National Intelligence, Febbraio 2022.
[236] P. Polityuk, J. Finkle, Ukraine says communications hit, MPs phones blocked, Reuters, 4 Marzo 2014. Accessibile a https://www.reuters.com/article/us-ukraine-crisis-cybersecurity/ukraine-says-communications-hit-mps-phones-blocked-idUSBREA231R220140304/
[237] K. Giles, Russia's 'New' Tools for Confronting the West - Continuity and Innovation in Moscow's Exercise of Power, Chatham House Research Paper, 2017.
[238] Ibidem.

paese, i paesi occidentali dovrebbero preoccuparsi per queste rinnovate capacità offensive russe. Di questo avviso è anche Andrew Lennon, ex comandante della forza sottomarina della NATO, il quale ha osservato che "la Russia è chiaramente interessata alla NATO e alle infrastrutture sottomarine dei paesi della NATO"[239].

Oltre alla presenza dei sottomarini, Rostelecom, la principale compagnia di telecomunicazioni statale russa, è stata coinvolta in numerosi attacchi che hanno deliberatamente reindirizzato il traffico Internet per spiare i dati in transito. Ad esempio, all'inizio del 2020, Rostelecom è stata coinvolta in "dozzine di potenziali dirottamenti" del Border Gateway Protocol, che funge da "GPS" di Internet per il traffico[240]. Poiché Rostelecom è impegnata in questa attività e per via dei suoi investimenti nei mercati internazionali per soddisfare il volume globale del traffico Internet, il comportamento e le pratiche dell'azienda trasformano "una falla di sicurezza nel centro dell'Internet globale, in un'arma micidiale"[241].

In definitiva, la Russia è stato uno dei primi stati a intravedere nei cavi sottomarini un'infrastruttura critica e pertanto un possibile obiettivo militare. In questo senso ha indirizzato gli investimenti con il fine di costruire una flotta adatta a questo scopo. Inoltre, a differenza di altri paesi, la Russia ha già dimostrato le sue capacità nel tagliare cavi sottomarini o nel reindirizzamento delle comunicazioni. A questi elementi, bisogna aggiungere anche la vicinanza geografica con l'Unione Europea ed i numerosi cavi sottomarini che si collegano poi agli Stati Uniti. In special modo, la Russia rappresenta una seria minaccia per tutti i cavi che passano per il Regno Unito.

3.2.2.2 La Cina

L'iniziativa cinese della Belt and Road Initiative (BRI), il cui obiettivo principale era la costruzione dell'attuale Via della Seta digitale (Digital Silk Road), è nata sulla sfiducia provocata dalle rivelazioni di Snowden circa le attività di spionaggio mondiale adottate da parte di Stati Uniti e Regno Unito[242]. La Cina si è dimostrata fortemente interessata al tema per differenti motivi: da una parte perché si tratta di un business che consente di aiutare i paesi in via di sviluppo a costruire delle infrastrutture essenziali in cambio di alleanze strategiche con questi paesi, dall'altra lo stesso funzionario di stato cinese ha chiaramente affermato che "Sebbene la posa di cavi sottomarini sia un'attività commerciale,

[239] M. Birnbaum, Russian submarines are prowling around vital undersea cables. It's making NATO nervous, Washington Post, 22 Dicembre 2017.
[240] Op. Cit. J. Sherman, Cyber Defense Across the Ocean Floor, pp.10.
[241] Ibidem.
[242] L. Burdette, Leveraging Submarine Cables for Political Gain: U.S. Responses to Chinese Strategy, Princeton University, JPIA, 5 Maggio 2021.

è anche un campo di battaglia in cui si possono ottenere informazioni"[243]. Lo scopo è quello di impadronirsi delle informazioni senza che queste debbano passare per le coste cinesi tramite i suoi landing spot.

La Cina sta attuando una politica intimidatoria nei confronti di Taiwan tramite azioni di guerra ibrida, tra cui vi rientra il dragaggio della sabbia. Questa azione può avere effetti dannosi non solo per l'intero ecosistema marino ma anche per il turismo dell'isola e soprattutto nei confronti dei cavi sottomarini che rischiano di essere danneggiati per via delle ancore dei pescherecci cinesi. Allo stesso tempo, si tratta di azioni di cui lo stato cinese può facilmente non prendersi la responsabilità e non abbastanza violente da giustificare una qualsiasi reazione da parte di Taiwan.

A differenza della Russia, la minaccia cinese è soprattutto di carattere commerciale. La forza delle aziende cinesi risiede nella loro capacità di offrire tariffe vantaggiose grazie ai sussidi di stato di cui beneficiano. Questo è il caso della HMN (in precedenza Huawei Marine Networks), azienda finanziata dalla Banca centrale cinese che si occupa di installare, riparare e costruire cavi, che ha proposto un'offerta del 20% inferiore rispetto ai concorrenti per la costruzione del cavo East Micronesia[244]. HMN ad oggi possiede il 10% dei cavi sottomarini e ha riparato il 25% dei cavi sottomarini globali[245].

La legge cinese sull'intelligence nazionale del 2017 ha imposto a tutte le aziende e cittadini cinesi di cooperare con i servizi di sicurezza. Questo pone seri dubbi circa la sicurezza dei cavi sottomarini gestiti da aziende cinesi. In questa cooperazione rientrano la condivisione di informazioni di identificazione personale, proprietà intellettuale, informazioni sulla sicurezza nazionale o qualsiasi altro traffico di dati rilevante[246]. Gli esperti sono quindi "giustamente preoccupati per l'inclusione di "backdoor" di spionaggio nell'infrastruttura Internet da parte di aziende cinesi, una politica che contraddice le migliori pratiche internazionali per la governance dei dati[247].

Gli USA sono stati a lungo preoccupati dall'attivismo cinese nel mercato dei cavi sottomarini. Nel 2020 questa preoccupazione si è concretizzata nella decisione della FCC di vietare il Pacific Light Cable Network che avrebbe unito gli USA ad Hong Kong. Questa decisione è stata presa in quanto il

[243] Geoffrey Starks, Statement of Commissioner Geoffrey Starks, U.S. Fed. Commc'ns Comm'n, pp.3, 2020. https://docs.fcc.gov/public/attachments/DOC-367238A6.pdf.
[244] R. Greene, P. Triolo, "La Cina controllerà l'Internet globale attraverso la sua via della seta digitale?" Fondo Carnegie per la pace internazionale, Sez.3, 8 maggio 2020.
[245] Op.Cit. Christian Bueger, Tobais Liebetrau, Jonas Franken, Security Threats to Undersea communications Cables and Infrastructure, pp. 38.
[246] Glick, Bonnie. 2020. Il futuro del 5G. Podcast. Donne intelligenti, potere intelligente. Centro di Studi Strategici e Internazionali, minuto 16.30. Accessibile a **https://www.csis.org/podcasts/smart-women-smart-power-podcast/future-5g** .
[247] J. Stavridis "China's next naval target is the internet's underwater cables". The Japan Times, 16 aprile 2019.

Dipartimento di Giustizia americano ha sostenuto che vi poteva essere una manipolazione delle informazioni di cittadini statunitensi che passavano tramite quel cavo in quanto alcuni punti di approdo si trovavano in paesi alleati della Cina ed il cavo stesso era in parte posseduto da un'azienda cinese che in quanto tale deve sottostare al controllo dello stato.

Le preoccupazioni da parte degli Stati Uniti sono state confermate anche da un documento Nato nel quale si sottolinea come "il governo degli Stati Uniti ha evidenziato il rischio di un'influenza dello Stato cinese su due fronti: la compromissione dei dati dei cavi attraverso i suoi proprietari (ad esempio, la raccolta di informazioni attraverso una CLS controllata dallo Stato) e cambiando la forma fisica di Internet per instradare più traffico globale attraverso la Cina (ad esempio, creando più punti di strozzatura nella rete globale sotto il controllo del governo cinese)[248].

3.2.4 Altre tipologie di attacco deliberato: gli attacchi digitali e le minacce al Network Management Systems

Dopo Stuxnet, è stata giustamente rinnovata l'attenzione su come proteggere le infrastrutture strategiche dai rischi posti dalla guerra informatica. I cavi, nonostante possano essere vettori di importanti attacchi digitali, sono stati sorprendentemente trascurati dal punto di vista della cybersicurezza.

Per danni di natura digitale si intendono quelle minacce che possono essere eseguite da remoto tramite l'hackeraggio dei Network Management System e interrompendo il flusso di dati e comunicazioni tra i landing spot ed i cavi sottomarini. Questi attacchi sono sottovalutati rispetto agli attacchi fisici ma stanno assumendo sempre più importanza da quando tutti gli operatori sono passati ad una gestione remota e digitale dell'infrastruttura. Non è un caso che il DHS statunitense abbia di recente sventato un attacco ad un cavo sottomarino alle Hawaii nel 2022 ad opera di un gruppo hacker[249]. L'avvento dei Remote Management Systems ha abbattuto notevolmente i costi ma ha aumentato le minacce di natura digitale su cui diversi attori hanno puntato l'attenzione. Basti pensare che l'hacker che nel 2022 aveva violato la sicurezza di una CLS delle Hawaii, in cui ha sede il Comando Indo-Pacifico degli USA, ci era riuscito grazie a delle credenziali ottenute tramite il dark web. Questo testimonia come mancasse una comune autenticazione a due fattori che è la regola principale di tutti i sistemi di cyber sicurezza oggigiorno.

Nell'attuale scenario industriale, in cui la transizione digitale diventa fondamentale per conseguire gli obiettivi di competitività e di efficienza produttiva, i "Sistemi di Supervisione, Controllo e

[248] Op.Cit, J. Sherman, 'Cyber Defense Across the Ocean Floor, p. 12.
[249] Bill Gertz, Threat to Undersea Cable in Hawaii Highlights danger of Future Internet Disruptions, The Washington Times, 22 ottobre 2022. Accessibile a https://www.washingtontimes.com/news/2022/oct/22/threat-to-undersea-cablein-hawaii-highlights-dang/.

Acquisizione Dati" (SCADA) rivestono un ruolo sempre più centrale. Essi, infatti, permettono di controllare in modo efficiente le apparecchiature o i processi industriali, raccogliere informazioni sulle prestazioni e trasmettere segnali di allarme o prendere decisioni rapide. Sono quindi assolutamente essenziali per migliorare le prestazioni della produzione industriale, ridurre i costi di manutenzione e aumentare la produttività[250]. Tuttavia, la digitalizzazione dei sistemi di diagnostica aumenta il rischio delle minacce cyber ed il loro impatto su tutto il sistema. A conferma di ciò, nel 2012 McAfee, la nota azienda specializzata in antivirus, sottolineava come questi sistemi introducessero "significative vulnerabilità in sistemi mai progettati per sostenere rischi di questo tipo"[251]. Negli ultimi anni, gli SCADA sono stati presi di mira, specialmente negli Stati Uniti, tanto da far affermare al segretario del Dipartimento di Sicurezza Nazionale, Janet Napolitano, che gli hacker erano sempre più vicini a mettere fuori uso diverse infrastrutture americane[252] come quelle che regolano la gestione delle acque reflue nei laghi o gli impianti di corrente dei centri commerciali[253]. Rispetto ai casi citati, i cavi sottomarini rappresentano un obiettivo altamente sensibile in quanto da essi dipende la gestione di interi settori dell'economia globale quali le transazioni finanziarie e la possibilità di accedere in sicurezza ai dati che le aziende archiviano tramite i servizi cloud.

Se gli SCADA sono utilizzati per la gestione fisica degli impianti delle infrastrutture, i Network Managment Systems (NMS) svolgono le stesse funzioni ma per le infrastrutture di rete. Quest'ultimi possono essere visti come l'interfaccia tramite cui si controllano i cavi sottomarini ed il loro funzionamento. Tramite i NMS gli operatori di rete possono controllare, ovunque siano nel mondo, ogni singola parte del cavo sottomarino come i ripetitori, le branching units, gli impianti di corrente e i punti di approdo. Come analizzato nel primo capitolo, una delle principali innovazioni nel campo della fibra ottica è stata quella del Multiplexing a divisione d'onda (WDM) che ha consentito di trasmettere più segnali ottici di diverse lunghezze d'onda attraverso un singolo cavo in fibra ottica aumentando così la capacità di trasmissione di dati del cavo. Per gestire il maggior traffico di rete si è fatto ricorso alla tecnologia ROADM (Reconfigurable Optical Add-Drop Multiplexer) che consente di aggiungere (add) o rimuovere (drop) specifiche lunghezze d'onda ottiche in modo flessibile e poter indirizzare così il traffico di rete nella destinazione che si

[250] F. Canna, SCADA: cos'è e come i sistemi SCADA migliorano l'industry 4.0, Network Digital 360, 5 Luglio 2023. Accessibile a https://www.innovationpost.it/tecnologie/automazione/sistemi-scada-cosa-sono-e-perche-sono-centrali-per-lindustry-4-0/
[251] Angela Moscaritolo, "A 'Critical' Turning Point: The Nation's Critical Infrastructure." SC Magazine, 3 Gennaio, 2012.
[252] Ed O'Keefe, "Janet Napolitano: Hackers Have 'Come Close' To Major Cyberattack," The Washington Post, 27 Ottobre, 2011.
[253] H. Hodson, "Hackers accessed city infrastructure via SCADA – FBI," Information Age, 29 Novembre, 2011.

preferisce[254]. Questa tecnologia è ciò che permette di reindirizzare il traffico tra i vari cavi qualora vi fosse un'interruzione di segnale oppure di interrompere la "la lunghezza d'onda blu sul canale 32" che corrisponde al fascio di luce che trasporta tutti i dati internet tra lo Yemen ed il Bahrain[255]. Un'intrusione nel Network Management Systems potrebbe permettere all'hacker di rendere invisibile un cavo sottomarino danneggiato all'operatore di rete semplicemente con uno switch di quel cavo da "red", che segnala un cavo danneggiato, a "green". Sostanzialmente, una volta dentro il sistema si ha il completo accesso alla rete comodamente da casa propria.

I motivi per cui questi sistemi risultano essere particolarmente fragili sono diversi a partire dal fatto che si appoggiano su sistemi operativi Windows e Microsoft che sono tra i più conosciuti dagli hacker e quindi tra i più facilmente attaccabili[256]. Inoltre, questi NMS sono direttamente connessi ad internet il che li rende un bersaglio ancora più visibile per gli hacker di tutto il mondo rispetto a quei sistemi che sono isolati e funzionano esclusivamente su reti locali[257]. Molti operatori si sono rivolti ai prodotti SCADA realizzata dalla Siemens che è risultata una delle aziende maggiormente colpite dal virus Stuxnet[258]. Diversi NMS, come quello prodotto dall'azienda NEC, permettono al singolo operatore di gestire fino a 1000 *Network elements* tra cui le *Line Terminal Equipment* (LTE) ed il *Power Feeding Equipment* (PFE) di più landing stations simultaneamente. Questo controllo avviene interamente da remoto tramite applicazioni che trasmettono i loro dati via internet e quindi tramite gli stessi cavi che devono gestire. Tra le varie fragilità si riscontra anche che tali software utilizzano sistemi operativi comuni e facilmente penetrabili come Linux (OS) e Microsoft Windows[259].

Tuttavia, il risparmio economico derivante dall'utilizzo di tali sistemi ha compensato il rischio che ne sarebbe derivato. Questo elemento risulta particolarmente emblematico del funzionamento dell'industria del settore che molto spesso è più attenta al profitto che ad implementare i massimi livelli di sicurezza possibili. Queste tematiche sono tenute sotto sorveglianza anche dagli stati ed infatti non è un caso che la seconda principale azienda che produce NMS sia Huawei Marine Networks. L'azienda sostiene di poter garantire alti livelli di sicurezza a costi assai ridotti. Anche in questo caso, si nasconde il dubbio che questi sistemi possano nascondere delle backdoor che

[254] OADM vs. ROADM: Qual è la differenza?, FOCC Fiber,4 Giugno 2019, Accessibile a https://it.fibresplitter.com/info/oadm-vs-roadm-what-s-the-difference-35913408.html
[255] M. Sechrist, New Threats, Old Technology – Vulnerabilities in Undersea Communications Cable Network Management Systems, Harward Kennedy School – Belfer Center, Febbraio, 2012, pp.25
[256] Ibidem.
[257] McAfee Labs, Threat Predictions, 2012. Accessibile a http://www.mcafee.com/us/resources/reports/rpthreat-predictions-2012.pdf
[258] Paul Roberts, "Siemens Working on Fixing Security Gap in Logic Controllers," ThreatPost: Kaspersky Lab Security News Service, 24 Maggio, 2011.
[259] Op.Cit M. Sechrist, New Threats, Old Vulnerabilities, pp.25.

faciliterebbero l'ingresso di hacker cinesi o della stessa Repubblica Popolare Cinese. Per tali ragioni gli Stati Uniti sono stati tra i primi paesi, insieme agli alleati australiani, a bloccare l'utilizzo di strumentazione prodotta da Huawei nei settori critici.

3.3 ATTIVITA' DI INTELLIGENCE E CAVI SOTTOMARINI

All'interno dell'UNCLOS si fa riferimento alla raccolta di informazioni ("Intelligence gathering"[260]) esclusivamente in un passaggio contenuto nella Parte II[261] relativa al "Mare Territoriale" ma questo non vuol dire che non sia stato un tema ampiamente trattato dagli stati nella preparazione della convenzione. Le posizioni degli stati sul tema erano diverse e lontane tra loro. Da una parte le potenze marittime miravano a rafforzare il più possibile il diritto di navigazione mentre i paesi costieri erano preoccupati che le flotte di paesi terzi potessero operare nelle loro acque nazionali e pregiudicare la sicurezza dei paesi costieri. Adesso si analizzeranno le sezioni dell'UNCLOS all'interno delle quali viene citato, direttamente o indirettamente, il tema della raccolta di informazioni. Dal punto di vista tecnico è importante sapere come i cavi sottomarini moderni possono essere utilizzati per più scopi, tra cui quelli di ricerca scientifica, monitoraggio delle calamità naturali e, per l'appunto, sorveglianza subacquea. Queste diverse attività vengono condotte mediante l'utilizzo di appositi sensori posizionati sui cavi come nel caso dei nuovissimi cavi sottomarini SMART[262][263]. Storicamente il metodo maggiormente utilizzato per la sorveglianza marittima è stato quello del cosiddetto Sound Surveillance System ("SOSUS") che a partire dagli anni 70, ha consentito alla US Navy di localizzare i movimenti dei sommergibili sovietici tramite il posizionamento di idrofoni disposti lungo un cavo in punti strategici che andavano a comporre delle lunghe posizioni di ascolto[264].

La sorveglianza elettronica ha una storia pluridecennale ed è stata è stata descritta come "una sorveglianza elettronica di massa (clandestina) da parte di uno Stato in tempo di pace delle comunicazioni di funzionari o cittadini di un altro Stato, quando queste comunicazioni avvengono in

[260] Le modalità con cui i cavi sottomarini possono essere utilizzati per attività di intelligence saranno analizzate nello specifico successivamente.
[261] UNCLOS, Art. 19 comma 2 lettera c, "qualsiasi atto volto a raccogliere informazioni a danno della difesa o della sicurezza dello Stato costiero" è considerato pregiudizievole per la pace, il buon ordine o la sicurezza dello Stato costiero e rende il passaggio non innocente.
[262] L' iniziativa Science Monitoring And Reliable Telecommunications (SMART) Subsea Cables mira a integrare sensori di temperatura, pressione e sismica dell'oceano nei sistemi di telecomunicazioni sottomarini commerciali che attraversano il fondale oceanico.
[263] M. Grabowski, Big boost for global network of SMART seafloor cables, early warning systems, University of Hawaii at Manoa, School of Ocean and Earth Science and Technology, December 15, 2021, Accessibile a https://www.soest.hawaii.edu/soestwp/announce/news/big-boost-for-global-network-of-smart-seafloor-cables-early-warning-systems/
[264] P. Mauri, Che cos'è il SOSUS, Inside Over, 22 febbraio 2021, accessibile a https://it.insideover.com/schede/guerra/che-cose-il-sosus.html

parte o interamente al di fuori del territorio dello Stato sorvegliante"[265]. Già a partire dagli anni 50 del secolo scorso gli Stati Uniti utilizzavano la sorveglianza elettronica non solo nei confronti degli stati ma anche verso i cittadini esteri e questa dinamica si è sempre più rafforzata negli ultimi anni. Ciò ha portato i cittadini a chiedersi se le loro comunicazioni fossero private o meno. Difatti in nome del concetto di "sicurezza nazionale" e grazie allo sviluppo delle tecnologie, le agenzie governative avevano dimostrato di aver allargato notevolmente il *range* di comunicazioni intercettate finendo per raccogliere dati che nulla avevano a che fare con l'interesse dello stato. Ad esempio, un recente leak ha rivelato che gli Stati Uniti stessero raccogliendo tutti i metadati telefonici e i contenuti delle chiamate effettuate alle Bahamas. Il motivo dichiarato era quello di concentrarsi su "trafficanti internazionali di stupefacenti e contrabbandieri stranieri di interesse speciale"[266] che pur rappresentando un crimine molto grave non rientra tra le priorità della sicurezza nazionale degli Stati Uniti.

Come già citato, all'interno delle acque territoriali la sovranità è del paese costiero e da ciò discende che ogni attività di raccolta di informazioni da parte di paesi terzi è proibita in quanto considerabile come un'azione che "arreca pregiudizio alla pace, al buon ordine e alla sicurezza dello Stato costiero"[267]. Chiaramente l'utilizzo dei cavi sottomarini con scopi di sorveglianza all'interno delle acque territoriali di un altro paese non è consentito dall'UNCLOS.

La Zona Economica Esclusiva rappresenta una via di mezzo tra le acque territoriali e l'Alto Mare ed è per questo che presenta alcune peculiarità. Questo difficile equilibrio di diritti insito nella ZEE ha creato numerosi dubbi sul fatto che la "raccolta di informazioni" tramite cavi sottomarini possa rientrare tra quelle attività permesse a Stati terzi nella ZEE che sono contenute nell'articolo 58 della convenzione. Inoltre è evidente che la sorveglianza o raccolta di informazioni sia un atto che potrebbe danneggiare la sicurezza nazionale dello stato costiero. A questa lettura si è sempre opposta quella delle potenze marittime, quali gli Stati Uniti, che hanno sostenuto come i principali diritti in capo agli stati costieri all'interno della ZEE sono di tipo economico, come suggerisce il nome stesso, mentre i diritti validi nell'Alto mare dovrebbero essere validi anche nella Zona Economica Esclusiva[268]. Non è un caso che proprio grazie ad una proposta degli Stati Uniti venne modificato il testo dell'art.58 e

[265] A. Deeks, An International Legal Framework for Surveillance, Virginia Journal of International Law, Vol. 55:2, pp. 299, 2015.
[266] Ryan Devereaux, Glenn Greenwald & Laura Poitras, Data Pirates of the Caribbean: The NSA Is Recording Every Cell Phone Call in the Bahamas, INTERCEPT (May 19, 2014), Accessibile a https://firstlook.org/theintercept/2014/05/19/data-pirates-caribbean-nsa-recording-every-cellphone-call-bahamas/
[267] Art. 58 comma 1, UNCLOS.
[268] R. Beckman, Submarine Cables – A Critically Important but Neglected Area of the Law of the Sea, 7° International Conference on Legal Regimes of Sea, Air, Space and Antarctica, Indian Society of International Law, New Delhi, 2010.

si aggiunse alla parola "libertà" un apposito riferimento incrociato all'articolo 87 (sulle libertà in alto mare)[269]. La Marina degli Stati Uniti ha espresso il concetto in modo molto chiaro sottolineando come l'esistenza della ZEE in un'area di operazioni navali non deve, di per sé, costituire una preoccupazione operativa per il comandante navale"[270]. In uno studio approfondito sull'argomento, Galdorisi e Kaufman affermano che la nuova formulazione, che amplierebbe la portata della disposizione così come apparsa originariamente, "era intesa a preservare i diritti di uso militare delle nazioni marittime nella [ZEE]"[271] Inoltre, tali paesi hanno sempre sottolineato come non si sia mai raggiunto un consenso tra i stati che hanno partecipato alla redazione dell'UNCLOS su questo tema. Tuttavia, le critiche a questa teoria sono molte a partire dal fatto che l'articolo 59 specifica come "gli Stati tengano in debito conto i diritti e gli obblighi dello Stato costiero" tra cui vi rientrano le sue prerogative di sicurezza nazionale che potrebbero essere lese qualora venissero attuate operazioni di sorveglianza all'interno della sua ZEE.[272]. Secondo diversi autori[273] la raccolta di informazioni nella ZEE sarebbe in contrasto con l'enunciato dell'art. 301 della Convenzione[274]. Il punto centrale è quindi determinare quando le attività di intelligence o raccolta di informazioni risultano come una minaccia o un uso vero e proprio della forza contro l'integrità territoriale del paese costiero. Ad oggi gli strumenti utilizzati nella cd. guerra elettronica (EW)[275] sono particolarmente elaborati e sono utilizzate con "scopi provocatori volti a generare risposte programmate"[276]. Altre attività SIGINT[277] intercettano radar ed emettitori navali, consentendo così la localizzazione, l'identificazione e il tracciamento delle navi di superficie, nonché la pianificazione e la preparazione di attacchi elettronici o missilistici contro di loro. Queste attività sembrano comportare un'interferenza molto maggiore con

[269] T.Davenport. (2015). Submarine cables, cybersecurity and international law: an intersectional analysis. *Catholic University Journal of Law and Technology, pp. 99.*
[270] Dipartimento della Marina, Manuale del comandante sulla legge delle operazioni navali , 1995, sezioni 2.4.2. e 2.4.3.

[271] Galdorisi,, Captain George V. USN (Ret.) and Kaufman,, Commander Alan G. JAGC, "Military Activities in the Exclusive Economic Zone: Preventing Uncertainty and Defusing Conflict," California Western International Law Journal: Vol. 32: No. 2, Article 4, 2002.
[272] T.Davenport. (2015). Submarine cables, cybersecurity and international law: an intersectional analysis. *Catholic University Journal of Law and Technology* , pp. 83.
[273] ibidem
[274] Art. 31, Unclos, "gli Stati contraenti si astengono dal ricorso alla minaccia od all'uso della forza contro l'integrità territoriale o l'indipendenza politica di qualsiasi Stato…"
[275] "La guerra elettronica comprende tutte le azioni nell'intero spettro elettromagnetico per intercettare, analizzare, manipolare o sopprimere l'uso dello spettro da parte del nemico e per proteggere l'uso amichevole dello spettro da attacchi simili da parte di un nemico.." Don.E. Gordon, Electronic Warfare: Element of Strategy and Multiplier of Combat Power, Pergamon, pp.192, 1981.
[276] Moritaka Hayashi, Military and intelligence gathering activities in the EEZ: definition of key terms, Marine Policy Volume 29, pp.123-137, Marzo 2005.
[277] "La SIGINT è l'intelligence derivata da segnali e sistemi elettronici utilizzati da obiettivi stranieri, come sistemi di comunicazione, radar e sistemi d'arma, che fornisce una finestra vitale sulle capacità, le azioni e le intenzioni degli avversari stranieri." National Security Agency, Signals Intelligence (SIGINT) Overview.

i sistemi di comunicazione e di difesa dello Stato costiero preso di mira rispetto a qualsiasi tradizionale attività passiva di raccolta di informazioni condotta dall'esterno del territorio nazionale[278]. Queste attività non implicano né l'uso della forza, né la minaccia della stessa come intese dall'articolo 58 dell'UNCLOS. Si tratta, tuttavia, di attività qualitativamente del tutto nuove e richiedono pertanto nuovi strumenti giuridici che ne limitino un uso spregiudicato.

La raccolta di informazioni in ambiente marittimo avviene principalmente in due modi: tramite sistemi composti da sensori dislocati sott'acqua (come nel caso del già citato SOSUS) oppure tramite l'intercettazione delle comunicazioni all'interno dei cavi sottomarini. In questo secondo caso si tratta di un'attività che richiede un intervento fisico sul cavo. Gli esempi di operazioni di questo tipo sono diversi come nel caso del sottomarino Jimmy Carter che nel 2005 era stato equipaggiato in modo tale da poter ascoltare le comunicazioni all'interno dei cavi sottomarini[279]. L'operazione prevede il "sollevamento del cavo dal fondale marino per essere portato all'interno del sottomarino, in una camera speciale dove l'equipaggio estrae i dati piegando la fibra o con la giunzione di una seconda fibra a ciascuna di esse"[280]. Pertanto, si tratta di attività di raccolta di informazioni che presuppongono un comportamento molto più attivo e potenzialmente dannoso rispetto a quello descritto nel caso dell'ascolto dei fondali marini tramite appositi sensori.

Resta da capire se l'UNCLOS è applicabile anche a questo particolare tipo di attività. Diversi esperti sostengono che i punti di maggior fragilità[281] del sistema sono le Cable Landing Stations[282]. Tuttavia si tratta di strutture che, pur controllando i cavi sottomarini, sono situate sulla terraferma mentre l'UNCLOS tratta esclusivamente comportamenti che si tengono sul dominio marittimo. Inoltre non è chiaro se questo tipo di sorveglianza possa rientrare sotto il concetto di raccolta di informazioni in ambiente marittimo che, come detto, mira a migliorare la conoscenza dell'ambiente marino e/o delle capacità militar delle marine di altri paesi. Al contrario, l'intercettazione fisica dei cavi sottomarini mira a raccogliere informazioni che travalicano il dominio sottomarino. Se si ritiene applicabile l'UNCLOS, operazioni di questo tipo, all'interno di acque territoriali, rientrano sicuramente tra quelle attività ritenute dall'articolo 85 come "passaggi offensivi" nelle acque di uno stato costiero. Infine per quanto concerne l'Alto Mare, la raccolta di informazioni rientra tra le attività permesse.

[278] Moritaka Hayashi, *Op. cit. a nota 51.*
[279] New Nuclear Sub is Said to Have Special Eavesdropping Ability, New York Times , 20 febraio 2005.
[280] T. Davenport, sopra nota 40, pp.49.
[281] Olga Khazan, The Creepy, Long-Standing Practice of Undersea Cable Tapping, The Atlantic, 16 Luglio 2013, Accessibile a https://www.theatlantic.com/international/archive/2013/07/the-creepy-long-standing-practice-of-undersea-cable-tapping/277855/
[282] Si tratta di un apposita scatola sotterrata dalla quale il cavo sottomarino può prendere direzioni diverse e dove sono disposti, solitamente, i ripetitori di segnale.

Da questa analisi sulla regolamentazione dell'attività di intelligence in ambiente marittimo emerge chiaramente come il diritto internazionale sia ignaro dell'esistenza dello spionaggio in tempo di pace o, per meglio dire, cerchi di ignorarlo. La poca chiarezza del diritto internazionale lascia la maggior parte della regolamentazione in mano alle leggi nazionali dei singoli paesi che disciplinano come e quali attività sono permesse agli stati esteri sul suo suolo. Per quanto concerne specificatamente l'UNCLOS, è possibile sottolineare come non vi fosse una piena volontà di regolamentare la raccolta di informazioni in ambiente marittimo. La mancanza di chiarezza rispetto al concetto stesso di "raccolta di informazioni" dimostra come i paesi ritenessero il tema rilevante ma mancasse una visione comune sulle modalità. Questa difficoltà si lega allo scontro di interessi tra stati costieri e stati terzi sui diritti di ognuno all'interno della ZEE. Le grandi potenze marittime ritenevano essenziale garantire la massima libertà di navigazione possibile mentre gli stati costieri più piccoli avevano paura di sentirsi costantemente accerchiati ed ascoltati. Se per molti anni il tema della regolamentazione della sorveglianza si era spostato sull'ambito strettamente cyber, oggi appare chiaro come i cavi sottomarini meritino una maggiore attenzione da parte del legislatore internazionale.

3.4 LE FRAGILITA' INFRASTRUTTURALI DEI CAVI SOTTOMARINI

In questo paragrafo vengono analizzati i rischi per i cavi sottomarini derivanti dalle fragilità insite nell'infrastruttura stessa. In questo caso si tratta di elementi che non rappresentano di per sé delle minacce, come nel caso dei rischi naturali, ma che possono amplificare eventuali attacchi al sistema o rendere più semplice prendere di mira l'infrastruttura in questione.

Bassa ridondanza di alcuni paesi: l'approccio della ridondanza[283] suggerisce che ogni Paese dovrebbe essere collegato verso l'esterno attraverso più cavi sottomarini, con l'obiettivo di limitare l'impatto economico e strategico negativo in caso di malfunzionamento o distruzione di singoli cavi[284]. Tale approccio fa sì che la rete di cavi di un paese possa contare su molteplici infrastrutture, in modo tale da minimizzare una singola possibile disfunzione [285]. Per semplificare, è possibile affermare che più cavi approdano in un paese e più questo è protetto da possibili attacchi alle sue linee di comunicazione. In tal senso, appare chiaro che gli stati insulari sono quelli più a rischio in quanto non possono contare sui collegamenti via terra ma la loro connessione in fibra passa

[283] In termini letterali, la ridondanza, nell'ingegneria dell'affidabilità, è definita come l'esistenza di più mezzi per svolgere una determinata funzione, disposti in modo tale che un guasto di un sistema possa verificarsi solo in conseguenza del guasto contemporaneo di tutti questi mezzi.
[284] A. Gili, Geoeconomia dei cavi sottomarini, ISPI, 27 gennaio 2022. Accessibile a https://www.ispionline.it/it/pubblicazione/geoeconomia-dei-cavi-sottomarini-33004.
[285] M. Patriarca, La sicurezza dei cavi sottomarini: una sfida per l'Europa, Geopolitica.info, 14 Ottobre 2021. Accessibile a https://www.geopolitica.info/cavi/.

unicamente attraverso i cavi sottomarini. La resilienza dei cavi dipende anche dal sistema di cavi sottomarini utilizzato. Il primo ad essere implementato per via della sua semplicità è stato il sistema lineare in cui il cavo unisce un punto A ad un punto B. In questo caso se il cavo viene danneggiato non vi è possibilità di reindirizzare il traffico in nessun modo. Questo sistema era quello comunemente utilizzato fino alla metà degli anni 90.

A partire dai primi anni 2000 si è diffuso il cosiddetto sistema ad anello (Ring Systems) per via della sua struttura circolare chiusa. Infatti, ciascun punto terminale del cavo è dotato di due collegamenti che si connettono a ciascun cavo nell'anello. Questo vuol dire che se ci sono quattro punti terminali, ci saranno otto connessioni totali. Questo permette al sistema di avere sempre due direzioni su cui instradare il traffico, una in senso orario ed una in senso antiorario. La Figura 2 è esemplificativa di quanto detto: una metà dell'anello si estende da Montreal ad Halifax fino a Southport mentre l'altra metà parte da Boston per arrivare prima ad Halifax e poi a Dublino. Per poter reindirizzare il traffico, ogni cavo è dotato di una parte di fibra ottica attiva (*lit capacity*) ed una parte inattiva (*dark capacity)* che viene utilizzata nel momento in cui si registra un guasto su una parte della linea. Sostanzialmente, ogni cavo è in grado di compensare la potenziale perdita di connettività di un cavo danneggiato. Questo sistema aumenta il grado di ridondanza di un sistema ma non elimina la possibilità che un cavo sia danneggiato ad entrambi i punti terminali del sistema. Inoltre, i costi di un sistema del genere sono maggiori vista la sua complessità.

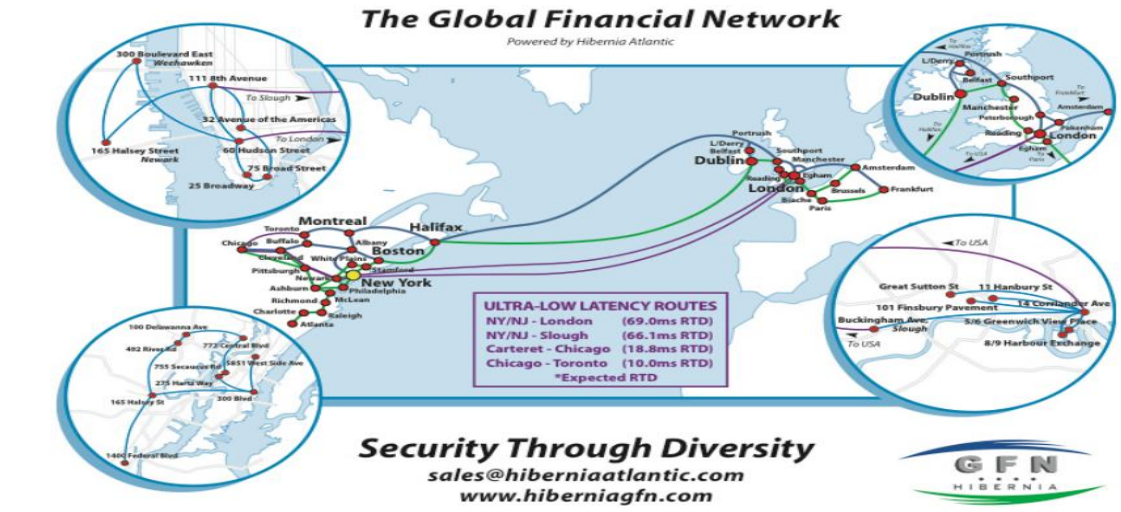


Figura 21: M. Sechrist, Cyberspace in Deep Water: Protecting Undersea Communication Cables, Harward Kennedy School, 2013.

Negli ultimi anni si è affermato un nuovo design di rete noto come Mesh Network. La differenza principale risiede nel numero di collegamenti esistenti per ciascun nodo. Come è possibile notare

dalla Figura 3, ogni CLS è collegata a diversi cavi che possono essere sia terrestri che sottomarini. Si tratta di un sistema con un alto livello di ridondanza ma allo stesso modo anche la sua complessità è maggiore rispetto ai sistemi precedentemente analizzati.

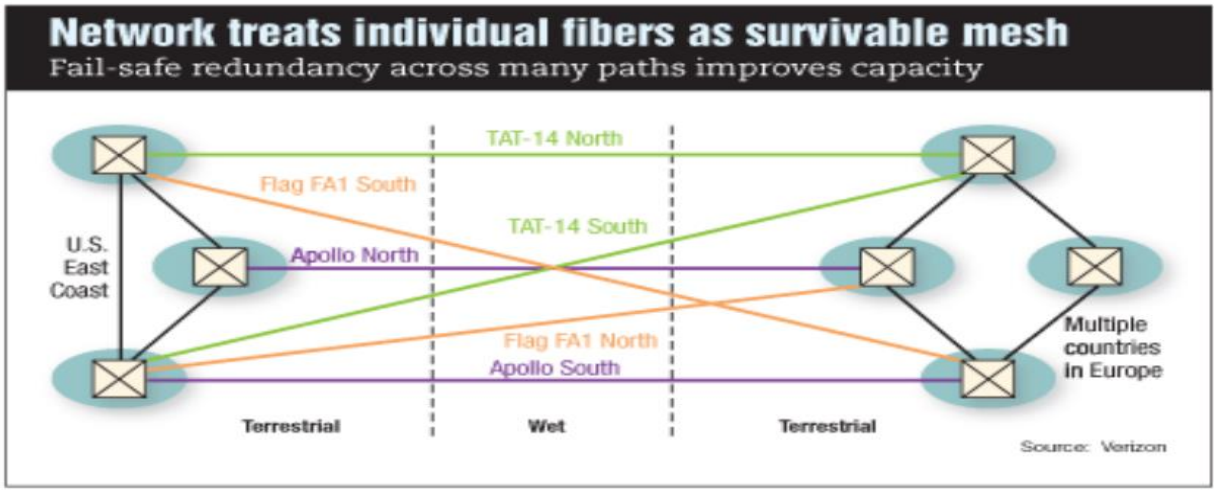


Figura 22: Dane Cooperson, "Undersea networks: Traffic growth and resiliency in the spotlight", 25 Maggio 2007.

Aldilà del sistema utilizzato, è soprattutto il numero di cavi di cui dispone un paese a fare la differenza. Ciononostante, anche i paesi sviluppati possono subire gravi perdite di connessione. Basti pensare all'India che nel caso di un taglio di tre cavi sottomarini, perderebbe il 70% della connettività con l'Europa[286].

La pubblicazione online delle rotte dei cavi sottomarini, comprese le cable landing station: il percorso dei cavi sottomarini è costantemente riportato dalle tre principali istituzioni idrografiche che emettono le carte nautiche mondiali: The National Oceanographic Data Center (DMA/NOAA) negli Stati Uniti, the Admiralty hydrographic office nel Regno Unito, and the Marine Hydrographic and Oceanographic Service (EPSHOM) in Francia. Queste rotte sono rese pubbliche in modo tale da evitare che i marinai gettino ancore o reti da pesca nelle zone adiacenti ai cavi sottomarini con il rischio di danneggiarli. Come è già stato fatto notare, questa mitigazione del rischio non è sufficiente ad evitare tale minaccia ma è sicuramente di aiuto. È possibile affermare che per fronteggiare quella che è la minaccia principale (il danneggiamento da parte dei mercantili), si aumenti il rischio di una minaccia considerata di minore rilievo ossia il danneggiamento volontario da parte dell'uomo.

[286] Lixian Hantover, If You Store Your Files in the Cloud, You Really Need to Be Worried About the Ocean, Huffington Post, 6 Dicembre 2017.

I colli di bottiglia sono uno dei maggiori rischi geografici per l'infrastruttura dei cavi. In ambito marittimo si è già sottolineato il ruolo dello Stretto di Luzon o dello Stretto di Gibilterra ma la medesima criticità è riscontrabile a terra. All'inizio e alla fine di ciascun cavo si trovano le landing stations dove troviamo sia gli impianti che danno l'energia ai cavi sia la strumentazione che consente ai cavi di instradarsi sui diversi percorsi in fibra ottica a terra. La sua funzione è quella di un crocevia. Il problema è che i cavi tendono a convogliare nelle stesse stazioni di atterraggio aumentando l'impatto di un singolo attacco nei confronti del sistema. Il caso degli Stati Uniti è uno dei più noti e sorprendenti. Secondo il ricercatore Micheal Sechrist, tutti i cavi transatlantici, eccetto uno, approdano in un raggio di 30 chilometri intorno a New York[287]. Addirittura, vi sono diversi operatori del settore che sostengono che tutti questi cavi passano sotto un singolo edificio nel centro di Manhattan, contraddicendo la credenza popolare secondo cui i paesi sviluppati possiedano un altissimo livello di ridondanza e resilienza del sistema[288]. Questa teoria è sostenuta anche da alcuni documenti divenuti pubblici tramite l'inchiesta Wikileaks che testimoniano come gli stessi Stati Uniti abbiano stilato una lista dei "punto di approdo" che rappresenterebbero delle infrastrutture situate all'estero critiche per la sicurezza nazionale degli Stati Uniti[289]. Da notare come si tratti di un'etichetta che solitamente possiedono solo le strutture militari[290]. Nonostante ciò, si riscontra un livello di sicurezza assolutamente inadeguato vista la funzione svolta da tali strutture. Questo è dimostrato in primis da un rapporto del "Centro per le infrastrutture protette del Regno Unito" che ha osservato nel 2006 che le stazioni di atterraggio dei cavi "sono relativamente scarse in termini di sicurezza fisica. In alcuni casi (ad esempio Land's End) il parcheggio è incontrollato e immediatamente adiacente all'edificio - un rischio evidente. L'accesso agli edifici presidiati avviene attraverso una tradizionale porta d'ingresso con telecamere a circuito chiuso anche se la sicurezza a questo livello dipende dai processi e dal modo in cui il personale della stazione gestisce i visitatori inattesi" [291]. A ciò si aggiunga che all'interno della struttura è possibile arrecare danni ingenti senza l'utilizzo di particolari strumenti ma anche solo tramite un'ascia, sempre secondo il report citato.

Come nel caso delle rotte dei cavi sottomarini, il problema è che vi è troppa pubblicità circa le posizioni di queste stazioni di approdo. Un esempio lampante è quello di una CLS che si trova in

[287] Op. Cit, Sechrist, 2013.
[288] Op. Cit, Sechrist, 2013.
[289] WikiLeaks (2009) 'Request for Information: Critical Foreign Dependencies (Critical Infrastructure and Key Resources Located Abroad)'
[290] Op. Cit, Undersea Cables, Policy Exchange.
[291] An Overview of the Use of Submarine Cable Technology by UK PLC, Centre for the Protection of National Infrastructure, Marzo 2006.

Egitto, per la precisione ad Alessandria. Vi basterà digitare le coordinate 31° 11.738' N, 29° 54.108'[292] per trovare l'edificio al di sotto del quale passano alcuni dei cavi trans-nazionali più importanti al mondo (FLAG, SEA-ME-WE 1, SEA-ME-WE 2, SEA-ME-WE 3 e l' AFRICA-1) che trasportano circa l'80% della connettività tra Europa e Medio Oriente[293]. Ciò che ancora più sorprende è che si tratta di informazioni riguardanti la sicurezza nazionale di un paese con tendenze autoritarie come l'Egitto e su cui spesso è difficile reperire informazioni. Non è un caso che nel 2013 le autorità egiziane abbiano arrestato tre subacquei che si trovavano sulle loro coste nelle vicinanze del cavo SeaMeWe-4, che trasporta un terzo dei dati tra Europa ed Egitto, con l'accusa di aver cercato di danneggiare il cavo in questione. Tuttavia, il governo del Cairo non ha mai fornito ulteriori informazioni lasciando un velo di mistero su tutta la vicenda. Alla luce di queste considerazioni, è possibile affermare che questi luoghi potrebbero essere degli obiettivi delle organizzazioni terroristiche come dimostrato da un attentato sventato da Scotland Yard, nel 2007, ad opera di Al-Qaeda ai danni di un Internet exchange situato a Londra. Queste strutture tendono a essere protetti fisicamente da recinzioni o filo spinato e da apparecchiature di sorveglianza a distanza, come telecamere e sensori[294]. L'ubicazione precisa di queste strutture non è di pubblico dominio, anche se esistono mappe indicative che potenzialmente possono renderle facile da identificare. Esiste infatti una "comunità di avvistamento" transnazionale delle stazioni di atterraggio che mira a fotografare le stazioni di atterraggio e a pubblicarne l'esatta ubicazione[295].

Mancanza di un **centro emergenza unico** che sia incaricato di individuare il danneggiamento di un cavo sottomarino (o a cui possa essere comunicato dalle CLS) e che predisponga immediatamente una risposta. Questo comporta che vi siano tempi spesso lunghi prima che le navi di riparazione possano intervenire in quanto gli stati possono tardare nell'approvazione delle autorizzazioni. La mancanza di un centro di questo tipo fa sì che gli Stati non possiedano dei sistemi di "Early Warning System" che possano prevenire o almeno individuare tempestivamente il danno. Questa mancanza di collaborazione tra stati costieri e aziende private è stata individuata anche da un rapporto dell'ICPC sul tema[296]. Inoltre, non bisogna dimenticare come le riparazioni di questi cavi

[292] Per la precisione l'edificio si trova all'incrocio tra El Horreya e El Nabi Streets ed è costruito dove una volta sorgeva l'antica biblioteca di Alessandria. A testimonianza dell'importanza di questo edificio, non è possibile visionarlo da vicino tramite l'estensione di Google Maps in 3D nota come Street View in quanto probabilmente ne è stata impedita la pubblicità dal governo egiziano. Tuttavia, come riportato da alcuni operatori di settore, si tratta di un edificio molto vecchio e con poca sicurezza (Hank Nussbacher, "Undersea Cables: Jan 20 IDC" IDC Seminar presentation, January 20, 2004. Accessed at http://www.interall.co.il/presentations/undersea-2004.pdf)
[293] Op. Cit, Sunak, Undersea Cables, Policy Exchange.
[294] Op.Cit, C. Bueger, T. Liebetrau, J. Franken, Security threats to undersea communications cables and infrastructure.
[295] Ibidem
[296] A. Niedbala, R. Berry, The Coast Guard Should Lead to Protect Undersea Cables, U.S Naval Institute, Vol. 149/8/1,446, Agosto 2023.

siano affidate interamente al settore privato sia perché essi ne sono i proprietari ma soprattutto perché sono gli unici che dispongono dei mezzi per poter realizzare tali operazioni. Un esempio lampante è quello degli Stati Uniti che non dispongono più di sottomarini di ricerca in immersione profonda come era l'NR-1[297]. Ad oggi, gli AUV (veicoli sottomarini autonomi) ed i sottomarini di ricerca con equipaggio sono esclusivamente di proprietà civile e non della Marina degli Stati Uniti[298]

Le navi per le riparazioni sono poche per affrontare un danneggiamento su scala globale dei cavi sottomarini come nel caso di un attacco deliberato. Il loro numero è commisurato ad affrontare i danni di natura accidentale che avvengono solitamente durante l'anno. Inoltre, spesso devono operare in condizioni estremamente complicate per via dei fenomeni naturali che colpiscono queste aree. Come è già stato affrontato nel primo capitolo, le riparazioni avvengono ad opera di imprese specializzate che stipulano dei cosiddetti "Maintenance & Repair Agreement" con i proprietari dei cavi in base ai quali queste aziende possono richiedere l'intervento di una nave per le riparazioni 365 giorni all'anno. Queste navi sono situate in porti strategici e sono sempre pronte a salpare. Per poter usufruire di questo servizio le aziende devono pagare una tassa annuale oltre ai costi necessari al singolo intervento come il carburante ed il costo della riparazione vera e propria. Per quanto riguarda l'Europa sono due gli accordi rilevanti, l' Atlantic Cable Maintenance & Repair Agreement (ACMA) ed il Mediterranean Cable Maintenance Agreement (MECMA). Secondo questi accordi, in Unione Europea sono dislocate 3 navi per le riparazioni che devono intervenire in un'area che va dal Mare del Nord al Mar Rosso. Pertanto, la capacità di intervento è più limitata di quanto sembri. Inoltre, è importante sottolineare come l'Italia sia uno dei paesi con il maggior numero di riparazioni effettuate in termini assoluti ed in special modo all'interno delle proprie acque territoriali. Quest'ultimo è un elemento significativo in quanto le riparazioni possono subire notevoli ritardi per via delle autorizzazioni che sono richieste dai diversi paesi per intervenire nelle proprie acque territoriali a differenza della Zona Economica Esclusiva che richiede un numero minore di permessi. Come dimostrato in figura 9, l'Europa è la zona con il maggior numero di operazioni di riparazioni (fatta eccezione per la Cina). Sempre secondo il dataset realizzato da SubOptic nel 2013, il paese dove si impiega più tempo per riparare i cavi sottomarini è l'Indonesia e

[297] 1 Robert W. Button, John Kamp, Thomas B. Curtin, and James Dryden, "A Survey of Mission for Unmanned Undersea Vehicles," (2009 RAND National Defense Research Institute), xviii.
[298] The Protection of Undersea Cables: A Global Security Threat, Commander M. Matis, United States Army War College, 2012.

la causa principale è da rinvenire nei permessi[299]. La Figura 10 mostra le zone con il maggiore ritardo nel realizzare le riparazioni a livello mondiale.

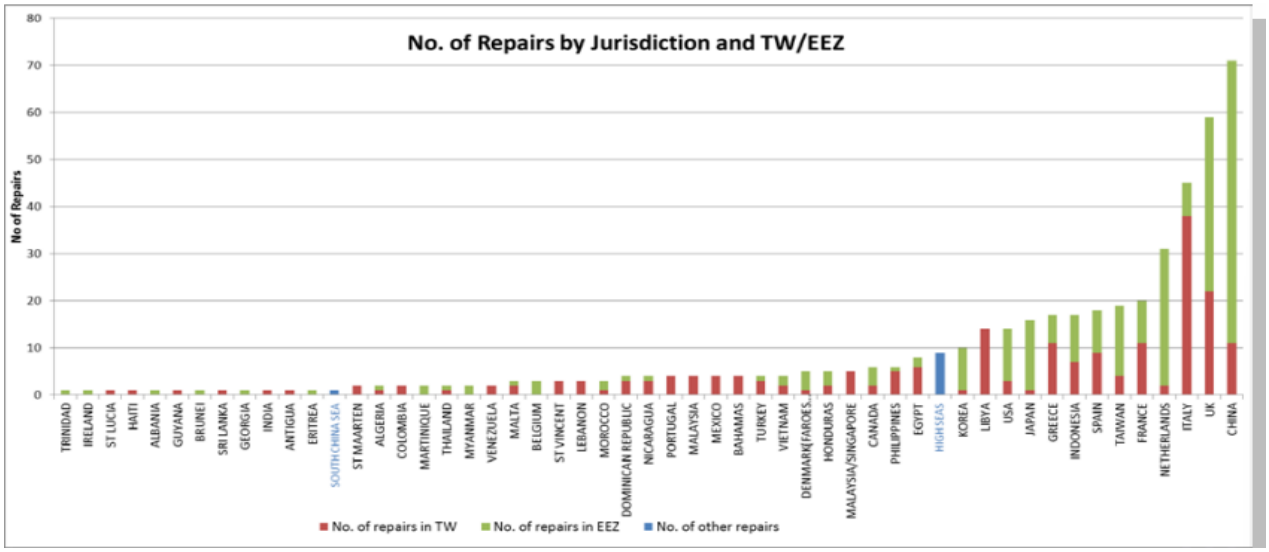


Figura 23: A. Palmer-Felgate, N. Irvine, S. Ratcliffe, MARINE MAINTENANCE IN THE ZONES – A GLOBAL, SubOptic, 2013.

In conclusione, è possibile affermare come il ridotto numero di navi da riparazione renda il sistema particolarmente fragile. Come sottolineato, in Europa vi sono solo 3 di queste navi (ed una in UK) e si trovano in dei porti civili dove non sono presenti gli stessi sistemi di sicurezza dei porti militari. In caso di un attacco coordinato nei confronti dei cavi e delle navi da riparazione, i tempi per far tornare online le comunicazioni sarebbero molto lunghi. In special modo se questi attacchi congiunti avvenissero in parti diverse del mondo con l'impossibilità per le altre navi esistenti di poter lasciare la propria area di appartenenza per soccorrere l'Europa.

[299] A. Palmer-Felgate, N. Irvine, S. Ratcliffe, and S. S. Bah, 'Marine maintenance in the zones: A global comparison of repair commencement times', Suboptic Conference: From Ocean to Cloud, 2013.

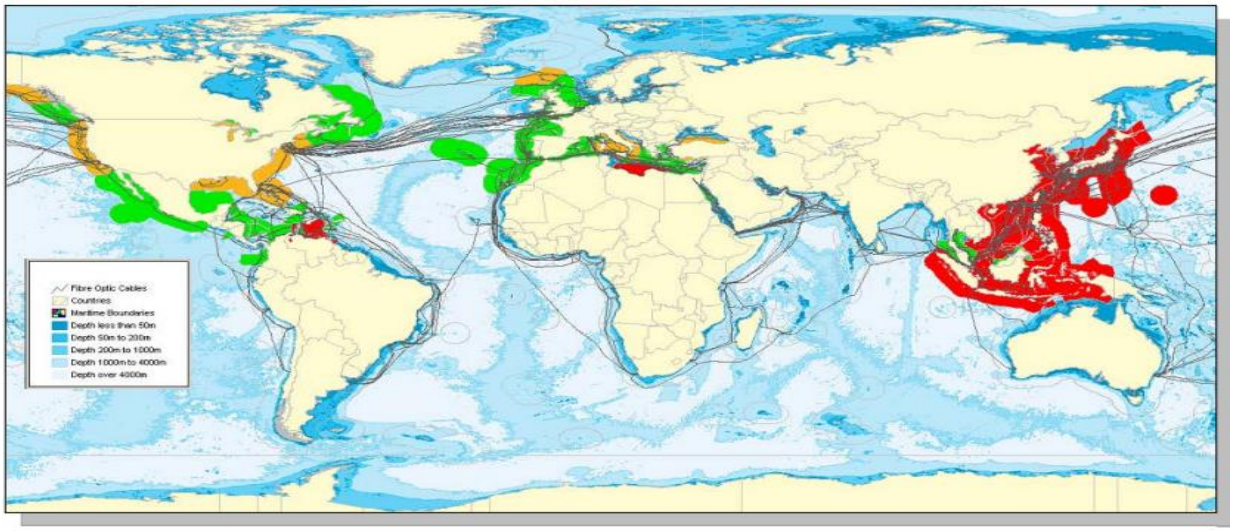


Figure 7: Coloured coded map showing mean notified to departure time for each jurisdiction.
Green = < 5 days, Orange = 5-10 days, Red = >10 days.

Figura 24: D. R. Burnett, Submarine Cables and the UNCLOS, Squire patton boggs. Accessibile a https://globaloceanforum.com/wp-content/uploads/2016/03/submarine-cables-and-unclos.pdf.

3.5 IMPATTO DELLE MINACCE E MITIGAZIONE DEL RISCHIO

Innanzitutto, bisogna sottolineare la mancanza di test di vulnerabilità e resilienza del sistema effettuati a livello internazionale (solo su scala nazionale)[300]. Pertanto, non possiamo sapere quali sarebbero le conseguenze globali di un simile attacco e come risponderebbe la comunità internazionale. Le stime che sono state effettuate sono del tutto approssimative e possono variare notevolmente da paese a paese.

Dal punto di vista economico, l'ICPC ha stimato che il taglio di un cavo sottomarino abbia un impatto finanziario di circa 1,5 milioni di dollari all'ora[301]. Tuttavia, si tratta di una stima che tiene conto solo delle perdite relative agli operatori o enti governativi che utilizzano la banda larga che passa per quel cavo per operazioni quotidiane ma non sono calcolati tutti i danni indiretti provocati dal rallentamento generalizzato di internet.

Anche i paesi maggiormente sviluppati possono essere fortemente colpiti dai danneggiamenti a dei cavi sottomarini. Un ambito in cui ciò è particolarmente evidente è quello militare. Difatti, è bene

[300] The International Cable Protection Committee (ICPC) website, "A Short History of Submarine Cables," Telstra Last modified: 28th September, 1998, http://www.iscpc.org/ information/History_of_Cables.htm (accessed December 19, 2011)
[301] Sechrist pp.38.

specificare come le comunicazioni militari non viaggiano su cavi sottomarini specializzati ma su quelli commerciali in cui viaggiano anche le nostre informazioni. Questo meccanismo rende più complicato estrapolare le informazioni sensibili del governo in quanto si tratta di cercare un ago in un pagliaio ma allo stesso tempo i cavi commerciali sono conosciuti e poco difesi. Per la Difesa si tratta di un trade-off di difficile soluzione. Un caso di studio cruciale è rappresentato da un incidente verificatosi nel dicembre 2008, quando tre dei più grandi cavi sottomarini del mondo che collegano l'Italia con l'Egitto, sono stati inconsapevolmente interrotti dal traffico marittimo nel Mediterraneo. Nel giro di poche ore, le interruzioni della connettività regionale avevano messo fuori uso l'80% della connettività tra Europa e Medio Oriente. Questo ha posto seri problemi operativi per le quasi 200.000 truppe britanniche e americane di stanza in Iraq in quel momento. Le più colpite sono state le forze aeree statunitensi, per le quali i veicoli aerei senza pilota (UAV), talvolta noti come droni, erano diventati uno strumento cruciale nelle operazioni antiterrorismo sia in Iraq che in Pakistan. Pilotati a distanza dall'Europa e dagli Stati Uniti, gli UAV necessitano di una larghezza di banda di 500 Mb per funzionare, velocità difficile da raggiungere senza una solida rete di cavi sottomarini.

3.5.1 Mitigazione del rischio

Nel corso di questo capitolo si sono passate in rassegna le principali minacce che colpiscono i cavi sottomarini. Queste fragilità son ben note sia al settore privato che ai policy maker tanto che nel corso degli anni sono state prese alcune misure per affrontare queste criticità. Pertanto, si vuole concludere il capitolo con una rassegna degli elementi che contribuiscono a mitigare i rischi citati. Molte delle politiche elencate nel paragrafo sono già state implementate mentre in altri casi si tratta di accorgimenti che sarebbe opportuno prendere in considerazione.

Pesca: per evitare i danneggiamenti da parte delle ancore, i cavi vengono costruiti con un'apposita armatura e, se necessario, sotterrati in modo da evitare che siano colpiti. Inoltre, organizzazioni non governative come l'Oregon Fisherman's Cable Committee aiutano le aziende a coordinarsi con i pescatori. L'istituzione di zone protette per i cavi rappresenta un elemento imprescindibile nella loro protezione, specialmente rispetto al rischio causato dalla pesca.

Spionaggio: La crittografia dei dati che passano nei cavi sottomarini è essenziale per evitare che questi siano estrapolati tramite attività di intelligence. Questo è l'unico metodo per poter mettere al sicuro i dati dal momento che una sorveglianza completa dell'infrastruttura risulta impossibile.

Attacchi da parte dei sottomarini: si tratta di una delle minacce più complicate da fronteggiare per ogni stato. Trattandosi di forze navali, la prima linea difensiva è rappresentata dai propri asset militari come sottomarini e cacciatorpedinieri. Tuttavia, un altro importante strumento di difesa è rappresentato dai robot subacquei autonomi che sono ricompresi tra gli UUV[302] e possono essere sia autonomi che azionati a distanza a seconda del compito che devono svolgere che può andare dal supporto navale, alla guerra antisommergibile fino alla riparazione degli stessi cavi sottomarini[303]

Aumentare la ridondanza: Innanzitutto è necessario costruire ulteriori punti di approdo e cavi sottomarini in modo da non dipendere da pochi cavi. A livello di design dell'infrastruttura è preferibile il passaggio definitivo a sistemi Mesch. In tal senso, sarebbe utile che i singoli paesi introducessero il sistema Mesch tra gli elementi necessari per ottenere l'autorizzazione a costruire un cavo sottomarino nel loro paese.

Attacchi digitali: Un elemento imprescindibile è l'implementazione di misure di sicurezza nelle landing station (telecamere, personale di vigilanza ecc) che siano all'avanguardia e adatte a proteggere delle infrastrutture critiche. Ad esempio, i proprietari dei cavi che atterrano in una CLS non possono avere accesso a tutta la struttura ma solamente al SLTE (Submarine Line Terminal Equipment) del proprio cavo in modo da evitare possibili interferenze. Inoltre, la FCC negli USA può richiedere che il Network Operations Centers che si occupa del monitoraggio e supporto di questi servizi sia dislocato in territorio americano e non in dei paesi considerati a rischio.

Come nel caso dell'accesso alla CLS, anche per il singolo cavo non è consentito un accesso completo all'architettura del sistema. I proprietari solitamente hanno il "controllo" esclusivamente della coppia di fibre di cui sono proprietari in modo da evitare eccessive interferenze ed eventuali azioni dannose su tutto il cavo. Sostanzialmente, si ragiona per compartimenti stagni.

Guasti tecnici: L'implementazione di alimentatori di riserva per garantire che vi sia sempre l'energia necessaria al funzionamento dei ripetitori. I sistemi di rilevamento automatico dei malfunzionamenti nei cavi risultano particolarmente utili per intervenire in modo tempestivo. In questo modo cavi stessi si trasformano in sensori sia lo studio dell'ambiente marittimo che come strumenti di sicurezza. Creazione di un **early warning systems**: l'importanza di identificare un'agenzia specializzata nel settore risiede anche nell'esigenza di poter sviluppare un centro di emergenza che monitori l'attività dei pescherecci tramite i loro GPS (AIS) in modo da poter

[302] Unmanned underwater vehicles.
[303] M. Santarelli, L'esercito dei droni subacquei: lo scontro Usa-Cina si sposta sotto i mari, Agenda Digitale, 17 Maggio 2022.

avvisare i pescherecci ogni qualvolta si trovino in zone limitrofe ai cavi sottomarini. Un controllo capillare dei movimenti dei natanti permetterebbe anche di poter identificare quali soggetti si sono mossi verso i cavi ignorando gli avvertimenti ricevuti dall'autorità in questione e quindi non scopi chiaramente ostili.

La minaccia degli **MIEDs**: Per mitigare questa minaccia è necessaria sia una maggiore sorveglianza marittima di superficie che una sorveglianza subacquea tramite appositi sensori posizionati sopra i cavi sottomarini che possano rivelare attività sospette. Per quanto concerne questa minaccia le risposte devono essere prevalentemente di natura militare come la sorveglianza aerea e navale delle zone protette. La minaccia della pirateria e degli ICDs: Una maggiore sorveglianza marittima tramite la guardia costiera, le navi militari e con l'ausilio dei mezzi satellitari in modo da individuare attività sospette da parte di imbarcazioni civili nei dintorni dei cavi sottomarini.

CAPITOLO 4

LA GEOPOLITICA DEI CAVI SOTTOMARINI

Uno dei temi maggiormente analizzati dalla geopolitica è la modalità con cui il potere si manifesta nello spazio. In questo senso lo sviluppo tecnologico è sempre stato un fattore determinante nel segnare dei cambi di paradigma sia per quanto riguarda gli equilibri di potere sia nel rapporto tra l'esercizio umano del potere e l'ambiente circostante. Come sosteneva F. Ratzel, lo sviluppo tecnologico non ha reso gli ambienti del potere meno vincolanti rispetto al passato per chi li abita e lì agisce, ma li ha rimodulati, interconnessi tra loro e soprattutto moltiplicati[304]. Difatti, negli ultimi decenni si è assistito ad una grande evoluzione dei domini fisici controllabili dall'uomo. In epoca moderna, la terra era concepita come il luogo dove dominava il potere statuale e l'ordine stabilito dal diritto in quanto era possibile stabilire confini certi. La terra è il luogo dove l'uomo stabilisce la sua residenza ed i suoi centri di potere motivo per cui la sua protezione è motivo di maggiori attenzioni rispetto all'ambiente marittimo. I limiti tecnologici hanno imposto una visione del mare orizzontale in cui si prendeva in considerazione esclusivamente la superficie d'acqua e non ciò che vi era sotto

[304] M. Marconi, Imperialismo, nazionalismo e colonie nell'opera di Friedrich Ratzel, in Bollettino della Società Geografica Italiana, 4/2011, pp. 555-570

di essa. Il mare era inteso come uno mezzo per poter controllare terre tra loro lontane ma non aveva un suo rilievo di per sé in quanto non possedeva risorse ed infrastrutture. La prerogativa degli stati era il controllo delle linee di comunicazione. Non sorprende che il diritto del mare sia una branchia del diritto internazionale e che si basi sul rispetto della libertà di navigazione: un concetto impensabile sulla terraferma in cui il potere statuale si estende su ogni centimetro a disposizione.

La dicotomia bidimensionale terra-mare non sembra più attuale. Nel corso dell'ultimo secolo, la tecnologia ha permesso all'uomo di estendere le sue attività in almeno altri tre ambienti: l'aria, lo spazio extra-atmosferico e il ciberspazio. L'aria ha caratterizzato la seconda metà del Novecento, sviluppata dalla potenza americana che vi ha costruito sopra il segno del suo primato. È in corso di sviluppo l'ambiente extra-atmosferico, che procede nonostante l'enorme difficoltà tecnologica che la sua esplorazione e occupazione comporta. L'ultimo nato, il ciberspazio, a partire dagli anni Novanta ha avuto una crescita esponenziale, fino a occupare una parte sempre più rilevante nell'equilibrio del potere globale[305]. La peculiarità di questi ambienti geopolitici è proprio quella di ignorare le caratteristiche fisiche del mare e della terra: gli aerei, i satelliti o gli attacchi informatici possono operare indipendentemente dal fatto che l'obiettivo si trovi sulla terra o sul mare. Tuttavia, la vera trasformazione nel rapporto tra mare e terra si deve al cambiamento nel modo di condurre la guerra. La concezione del mare come "colonna d'acqua" e non più in senso orizzontale è stata possibile grazie allo sviluppo dei sottomarini. Inoltre, le navi militari hanno sviluppato sempre più maggiori capacità missilistiche permettendo di lanciare attacchi sulla terraferma (deep strike) e operazioni speciali direttamente dal mare[306]. Se in epoca moderna la superpotenza era quella talassocratica, oggi è necessario possedere un'attitudine anfibia che consenta di proiettare il proprio potere utilizzando il mare come piattaforma invece che come un "ponte" e quindi una mera linea di comunicazione. Questo cambiamento geopolitico si è concretizzato anche sotto l'aspetto normativo tramite l'estensione delle acque territoriali alle 12 miglia e l'istituzione della ZEE che hanno permesso agli stati di esercitare il proprio controllo e potere sulla colonna d'acqua e il fondo e sottofondo marino fino alle 200 miglia[307].

Queste dinamiche fanno parte della cosiddetta territorializzazione del mare[308] che si concretizza con la progressiva appropriazione, divisione e produzione degli spazi marittimi. È proprio quest'ultimo elemento che più rileva per tale studio. Difatti, se l'ambiente marittimo non nascondesse delle risorse

[305] Civiltà del mare - Geopolitica, strategia, interessi nel mondo subacqueo. Il ruolo dell'Italia, Fondazione Leonardo, Marina Militare Italiana, 7 marzo 2023, pp.16.
[306]Gli esempi più rappresentativi sono la Guerra del Golfo nel 1991, l'intervento NATO nella ex-Jugoslavia (1999), Enduring Freedom in Afghanistan (2001), le operazioni USA in Iraq (2003), Unified Protector e infine la Guerra in Siria alla quale i sottomarini russi della Flotta del Mar Nero.
[307] Ivi, pp. 18.
[308] G. De Ruvo, Cosa sono le Zone Economiche Esclusive e come i Paesi si stanno spartendo i confini del mare, GeoPop, 10 gennaio 2023. Accessibile a https://www.geopop.it/zone-economiche-esclusive-cosa-sono-significato/

di strategiche per gli stati, questi non avrebbero alcun interesse a sviluppare tecnologie che ne permettano il controllo. Le attività economiche che possono svolgersi sott'acqua sono relative innanzitutto al transito di cavi e ai dotti di collegamento, tanto per il passaggio di informazioni della rete di internet, che degli idrocarburi e dell'energia elettrica. Nessun altro ambiente geopolitico è così determinante in connessione con gli altri e al tempo stesso però esposto a pericoli per la sicurezza come quello subacqueo. I cavi sottomarini rappresentano le vie di comunicazione moderne. È tramite questa infrastruttura che gli esseri umani possono interagire a migliaia di chilometri di distanza e non sorprende che gli stati abbiano un interesse ad esercitare il proprio controllo su di esse. Ciò è amplificato dal fatto che queste comunicazioni non solo possono essere bloccato ma anche spiate e manomesse. I cavi sono una perfetta rappresentazione della potenza ibrida a cui si faceva riferimento. I centri di potere risiedono ancora sulla terraferma ma necessitano di un'infrastruttura subacquea per poter funzionare. In tal senso, sono funzionali alla proiezione del potere oltre oceano in quanto consentono il controllo delle informazioni e allo stesso tempo di poter stringere accordi bilaterali con i paesi in via di sviluppo che necessitano di queste infrastrutture. Pertanto, non sorprende che Cina e Stati Uniti stiano combattendo quella che è una guerra commerciale, tecnologica e militare che possiede somiglianze con la guerra fredda sebbene vi siano anche delle differenze sostanziali. In questo quadro si deve aggiungere l'approccio russo che si basa sulla forza militare ed utilizza il controllo dei cavi sottomarini per attuare la sua dottrina preferita: la guerra ibrida.

In questo capitolo si analizzeranno nel dettaglio le traiettorie che stanno perseguendo le tre grandi potenze e come queste si intersecano tra loro. L'obiettivo è quello di individuare i possibili risvolti per la sicurezza globale. Trattare il ruolo di questi paesi e la visione a medio termine che hanno sui cavi sottomarini sarà cruciale per poter individuare il ruolo dell'Europa, dell'Italia ed i relativi rischi per la sicurezza nazionale nel capitolo successivo.

4.1 LA POTENZA COMMERCIALE CINESE

La Cina tratta i cavi sottomarini non come un bene globale e di conseguenza neutro ma come delle risorse strategiche da poter sfruttare in caso di conflitto[309]. Risorse su cui la Repubblica Popolare Cinese vuole fortemente investire come testimoniato dal piano "China Manufacturing 2025" secondo cui Pechino punterebbe a controllare il 60% dei cavi[310]. Si tratta di un'inversione di tendenza che ha

[309] J. Kraska, "Tillerson Channels Reagan on South China Sea. Lawfare (blog), 12 gennaio 2017. Accessibile a https://www.lawfareblog.com/tillerson-channels-reagan-south-china-sea .
[310] F. Pani, Cavi sottomarini: Nuovo fronte caldo nella sfida tra USA e Cina, IARI, 6 Aprile 2023. Accessibile a https://iari.site/2023/04/06/cavi-sottomarini-nuovo-fronte-caldo-nella-sfida-tra-usa-e-cina/ .

avuto inizio in seguito alle rivelazioni di Swoden sull'intercettazione delle comunicazioni civili ad opera di Stati Uniti e Regno Unito. Cina e Russia hanno subito capito che si fosse aperta una falla di credibilità nel blocco occidentale e che si trattasse dell'occasione perfetta per emergere come capofila di una nuova governance di internet e delle comunicazioni. La Cina non mirava ad ottenere le simpatie dell'opinione pubblica europea ma ad accreditarsi come player credibile nei confronti dei paesi del Sud del mondo. Le conseguenze furono immediate: il Brasile annunciò immediatamente di volersi rendere indipendente dai cavi sottomarini con gli Stati Uniti grazie alla costruzione del cavo BRICS che sarebbe dovuto passare per il Sud Africa, l'India, la Cina e la Russia. Sebbene questo progetto non si sia mai realizzato, si è trattato di un primo tassello del nuovo puzzle. Il settore dei cavi è stato scosso violentemente dalla strategia della Digital Silk Road.

4.1.1 Digital Silk Road

La Digital Silk Road si è presentata come un'alternativa alle tecnologie dell'informazione e della comunicazione (ICT) statunitensi con lo scopo di aiutare a migliorare le reti di telecomunicazioni straniere, l'intelligenza artificiale, il cloud computing e le capacità di sorveglianza[311]. La DSR è una direttiva politica vagamente definita diretta da forze sia dal basso verso l'alto che dall'alto verso il basso che confondono i confini tra strategia pubblica e azione privata[312]. La Cina ha introdotto il programma nel 2015, lo stesso anno in cui era previsto il completamento dell'ormai fallimentare cavo BRICS. Attraverso il DSR, "le aziende cinesi hanno silenziosamente eroso il dominio statunitense, europeo e giapponese sul... mercato dei cavi sottomarini"[313]. Tuttavia, sbarcare in Cina o essere posseduti da aziende cinesi potrebbe non essere più sicuro della tecnologia statunitense che sperano di sostituire. La vaghezza della DSR rende molto complicato rintracciare i dati sulla sua espansione. Secondo alcuni analisti, a partire dal 2019, oltre il 70% delle nazioni africane e dell'Unione africana hanno firmato memorandum d'intesa (MOU) con Pechino sulla BRI[314].

4.1.2 Il cavo PEACE ed il Progetto Cina-Pakistan in Fibra Ottica (CPFOP)

La Cina vede nei cavi sottomarini un asset strategico non tanto per lo sviluppo interno del paese ma soprattutto come elemento di proiezione della sua potenza. In questo senso, la BRI indica le aree su

[311] Kurlantzick, Joshua, and James West, "Assessing China's Digital Silk Road Initiative", Council on Foreign Relations, 2021.
[312] Ang, Yuen Yuen, "Demistificare Belt and Road: la lotta per definire il 'progetto del secolo' della Cina". Foreign Affairs, 22 maggio 2019. Accessibile a https://www.foreignaffairs.com/articles/china/2019-05-22/demystifying -B… .
[313] Tobin, Meaghan, "Next Battleground in US-China Tech War: Undersea Internet Cables." South China Morning Post, sec. This Week in Asia, par. 3, 14 Dicembre 2019.
[314] Dahir, Abdi Latif, "These Are the African Countries Not Signed to China's Belt and Road Project." Quartz Africa, Par. 2, 30 Settembre 2019.

cui la Cina è intenzionata ad espandere la sua influenza. Per capire concretamente come la strategia cinese viene applicata, è possibile analizzare due progetti esemplificativi: il cavo PEACE ed il Progetto Cina-Pakistan in fibra ottica. Innanzitutto, entrambi trovano applicazione nella direttrice che unisce la Cina al Sud Est Asiatico e poi all'Africa e l'Europa. Un ruolo chiave lo gioca il Pakistan per due principali ragioni: la posizione geografica che situa il paese al centro dell'Oceano Indiano Occidentale e per il rapporto storico di conflitto con l'India che è la principale potenza regionale ed è oggi considerabile una potenza mondiale[315]. In questo senso il Pakistan gioca un ruolo di cuscinetto nei confronti di un paese che Pechino deve controllare per mantenere la sua influenza nella regione dell'Indo-Pacifico. La strategia ha sempre bisogno di uno strumento per poter essere resa operativa. Sul piano tattico i cavi sottomarini rappresentano lo strumento ideale sia perché si tratta di un'infrastruttura di cui il Pakistan ha bisogno e soprattutto perché sono un'arma di spionaggio utilizzabile anche nei confronti dei vicini Indiani i cui dati potrebbero passare attraverso tali cavi.

Il cavo Pakistan & East Africa Connecting Europe (PEACE), come dice il nome stesso, ha l'ambizione di connettere Cina, Africa ed Europa passando per punti di approdo direttamente controllati da Pechino tra cui il porto di Gwadar (di proprietà dell'azienda stalate China Overseas Ports Holding Company) e la città di Gibuti dove si trova la prima importante installazione militare estera cinese[316].

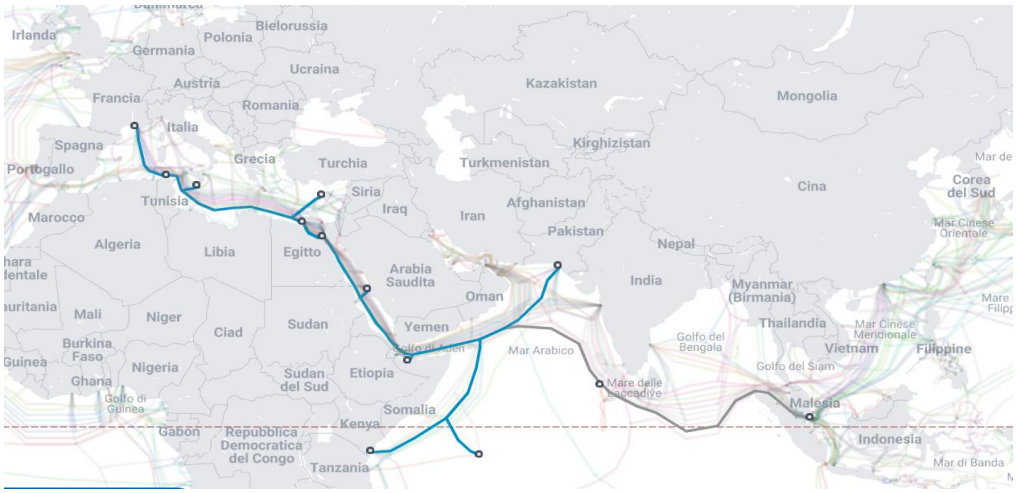


Figura 25: Fonte: TeleGeography, "Submarine Cable Map. PEACE Cable." Accessibile a https://www.submarinecablemap.com/submarine-cable/peace-cable

Come è visible in Figura, il cavo si estende lungo la costa Africana fino al suo punto di approdo finale a Marsiglia. Il cavo ha una lunghezza totale di 25.000 km e rappresenta la via di comunicazione più

[315] G. Gagliano, Cina: la Geopolitica dei Cavi Sottomarini, Notizie Geopolitiche, Qui Oriente, 19 Novembre 2023. Accessibile a https://www.notiziegeopolitiche.net/cina-la-geopolitica-dei-cavi-sottomarini/ .
[316] Il PEACE cable passa per i seguenti paesi:Cipro, Egitto, Francia, Kenya, Maldive, Malta, Pakistan, Arabia Saudita, Seychelles, Singapore, Somalia, Tunisia.

rapida tra Asia ed Africa per quanto riguarda le rotte di cavi sottomarini. Il cavo PEACE si inserisce all'interno del più ampio "Corridoio Economico Cina Pakistan" (CPEC) che prevede la costruzione di numerose infrastrutture nel tratto che unisce il porto di Gwadar con la città di Kashgar (Cina) per un valore totale che si aggira tra i 27 ed i 62 miliardi di dollari[317]. Una delle componenti del CPEC è rappresentata dal Progetto Cina-Pakistan in Fibra Ottica (CPFOP) che dovrebbe soddisfare la domanda di fibra di 17 milioni di persone.

La sicurezza nazionale e gli interessi statali sono due parametri importanti per la partnership tra tutti i paesi del mondo. Oltre ai vantaggi offerti dal CPEC, ci sono molte preoccupazioni sui termini dei contratti e sulla possibilità che questi possano deteriorare l'industria e persino la sovranità del Pakistan. Secondo gli esperti, le gare d'appalto attorno al CPEC favoriscono notevolmente Pechino. Ulteriori preoccupazioni riguardano le migliaia di acri di terreno agricolo affittati a imprese cinesi per sviluppare varietà di sementi e tecnologie di irrigazione.

Figura 26: Y. Ali, M. Asees Awan, A. Petrillo Et Al., Risk assessment of China-Pakistan Fiber Optic Project (CPFOP) in the light of Multi-Criteria Decision Making (MCDM), Advanced Engineering Informatics, Volume 40, 2019, Pages 36-45

Inoltre, vengono affidati ad aziende cinesi contratti per alcuni progetti di sicurezza nazionale, come l'installazione di un sistema completo di monitoraggio e sorveglianza nelle città da Peshawar a Karachi e la costruzione di una rete nazionale di Fibra Ottica per potenziare l'accesso a Internet. Se da una parte vi sono queste preoccupazioni, dall'altra è necessario sottolineare come il Pakistan necessiti di questo tipo di infrastrutture se si pensa che le sue comunicazioni passano tramite 5 cavi sottomarini situati a Karachi. Inoltre, il Pakistan si trova a metà strada tra i due principali colli di

[317] M. Afzal, "At all costs": How Pakistan and China control the narrative on the China-Pakistan Economic Corridor", Brookings, Research, Giugno 2020.

bottiglia del sistema che sono lo stretto di Malacca ed il Canale di Suez. Ciò comporta che tutte le sue comunicazioni devono obbligatoriamente passare per delle rotte particolarmente fragili.

I massicci investimenti della Cina in Pakistan, tuttavia, hanno sollevato preoccupazioni circa lo stress debitorio del paese. Secondo il Centro per lo sviluppo globale, il Pakistan ha un rischio "alto" di stress debitorio, in gran parte a causa della sua incapacità di ripagare i prestiti BRI[318]. Nel suo ultimo rapporto sul paese, l'FMI ha stimato il debito totale del Pakistan nei confronti della Cina a 18,43 miliardi di dollari alla fine dell'anno fiscale 2020/21, una quota significativa del suo debito estero totale di 91,77 miliardi di dollari[319]. L'incapacità di ripagare la Cina per i progetti infrastrutturali tanto necessari potrebbe dare a Pechino influenza sulle finanze, sull'economia e sulla politica di Islamabad.

Gli altri punti cruciali della strategia cinese sono Gibuti e l'Egitto. La loro importanza si deve in primis dalla loro posizione geografica. Gibuti è ben posizionato per gestire le comunicazioni e il commercio tra l'Oceano Indiano e il Mar Rosso e il Mediterraneo. Difatti, gli stati che si affacciano sul Golfo di Aden e all'ingresso del Mar Rosso sono diventati un luogo naturale per le stazioni di approdo delle informazioni che viaggiano attraverso l'EMEA. Per tali ragioni, la città di Gibuti è quella dove approda il maggior numero di cavi tra quelli che attraversano lo stretto di Bab El-Mandeb[320]. La zona del Canale di Suez, già un importante punto di transito per il commercio internazionale, è diventata fondamentale per le comunicazioni internazionali attraverso i cavi in fibra ottica tanto da ospitare il maggior numero di cavi tra i paesi dell'area MENA[321]. La Cina ne è ben consapevole ed ha investito notevoli risorse sull'ammodernamento tecnologico del paese sia a livello di infrastrutture che di capitale umano. Huawei ha formato oltre 5.000 professionisti egiziani delle tecnologie dell'informazione e della comunicazione (ICT) in quattro diversi centri, ha costruito il primo "OpenLab" – una piattaforma Internet of Things – al Cairo e ha introdotto soluzioni ICT per città intelligenti[322].

[318] Ghafar, Abdel Abdel. Jacobs, Anna L.. "Pechino chiama: valutare la crescente impronta della Cina nel Nord Africa". *Brookings* , 23 settembre 2019. https://www.brookings.edu/research/beijing-calling-assessing-chinas-growing-footprint-in-north-africa/

[319] Pakistan: 2021 Article IV Consultation, Sixth Review Under the Extended Arrangement Under the Extended Fund Facility, International Monetary Fund, Country Report No. 2022/027, 4 Febbraio 2022.

[320] T. Blaubach, Connecting Beijing's Global Infrastructure: The PEACE Cable in the Middle East and North Africa, Middle East Institute, 7 Marzo 2022. Accessibile a https://www.mei.edu/publications/connecting-beijings-global-infrastructure-peace-cable-middle-east-and-north-africa.

[321] Ibidem.

[322] Ibidem.

4.1.3 L'espansionismo cinese nel Mar Cinese Meridionale

I cavi sottomarini sono di cruciale importanza non solo nell'ottica di proiezione della potenza cinese in altri continenti ma anche nel proprio cortile di casa: il Mar Cinese Meridionale. Si tratta di un'area in continua crescita economica che già oggi ospita un terzo di tutto il traffico marittimo per un volume di scambi commerciali pari a 5.000 miliardi di dollari all'anno e che potrebbe arrivare a produrre un totale di 130 miliardi di barili di petrolio nel prossimo futuro. L'aggressività cinese in questo mare deve essere letta anche rispetto all'intenzione di impadronirsi dei dati che vi passano al suo interno. Si è analizzato nel capitolo precedente come l'UNCLOS risulti spesso ambigua rispetto ai poteri degli stati costieri nella ZEE ed è per questo che la Cina cerca di estendere il più possibile il confine della sua Zona Economica Esclusiva tramite la "linea a 9 trattini"[323] sostenuta da Pechino[324]. Difatti, in caso di danneggiamento di un cavo, i permessi per ripararlo devono essere richiesti allo stato costiero. Ritardare intenzionalmente i processi di riparazione dei cavi è illegale secondo l'UNCLOS, anche se questo da solo potrebbe non limitare le azioni della Cina[325]. Le autorità cinesi non solo hanno reso lungo e oneroso il processo per ottenere i permessi entro le 12 miglia ma hanno anche iniziato a richiedere i permessi per la posa di cavi nelle acque territoriali rivendicate oltre le 12 miglia. L'estensione dei confini marittimi garantirebbe alla Cina di spiare più facilmente i cavi che passano per le proprie acque (la quasi totalità) e contemporaneamente vietare il passaggio a sottomarini stranieri che potrebbero aver lo stesso obiettivo.

È interessante notare che le isole artificiali cinesi nel SCS possono fare affidamento su un gruppo separato di cavi che non compaiono sulle mappe pubbliche come segnalato da Reuters nel 2016 e da Long nel 2020. In questo modo la Cina potrebbe rendersi indipendente dai cavi sottomarini che collegano i paesi intorno a lei.

[323] Macias, Amanda,"L'Aia ha appena respinto la "Linea a 9 trattini" di Pechino nella sentenza sul Mar Cinese Meridionale". Business Insider, 12 luglio 2016.
[324] la sovranità cinese su questa porzione marittima, tratteggiata negli Anni 70 dall'allora premier Zhou Enlai, non è internazionalmente riconosciuta ma anzi contestata da vari Stati affacciati sul Mar Cinese Meridionale, come Vietnam, Malesia, Filippine e Brunei. Vedi F. Pani, Cavi sottomarini: nuovo fronte caldo nella sfida tra Usa e Cina, IARI, 6 Aprile 2023. Accessibile a https://iari.site/2023/04/06/cavi-sottomarini-nuovo-fronte-caldo-nella-sfida-tra-usa-e-cina/.
[325] L. Burdette, Leveraging Submarine Cables for Political Gain: U.S. Responses to Chinese Strategy, Princeton, Journal of Public e International Affairs, 5 maggio 2021.

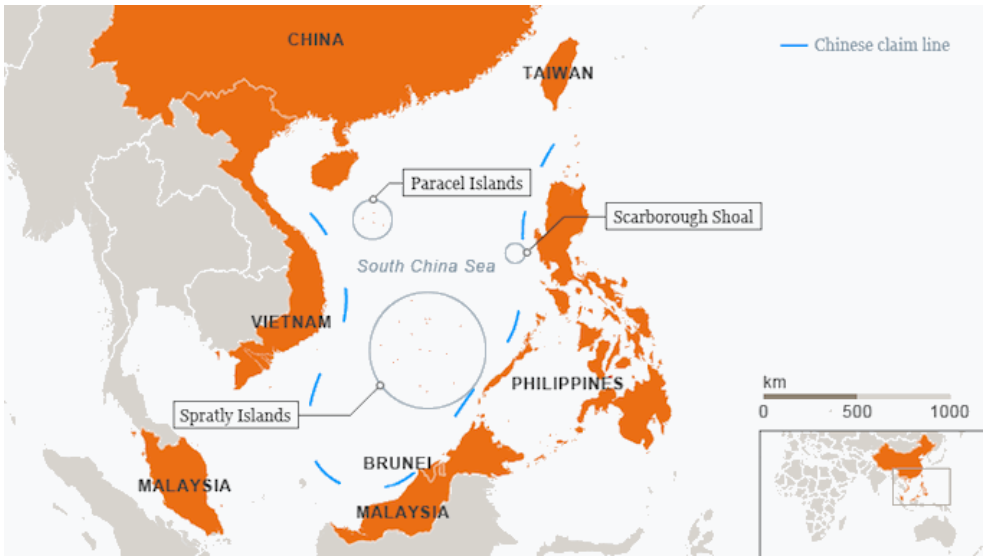


Figura 27: R. Casadei, Il conflitto Cina-Usa si sposta sulla "Linea dei 9 trattini", Tempi, 7 Maggio 2020.

4.1.4 Rimodellare internet tramite le aziende: la strategia cinese e russa

Gli stati possiedono molteplici interessi nell'ambito dei cavi sottomarini. Da una parte vi è l'intento di costruire più punti di approdo possibili nel proprio territorio in modo da aumentare il grado di resilienza del proprio sistema. Si tratta di uno scopo puramente difensivo. Tuttavia, come è stato più volte sottolineato, i cavi sottomarini sono anche un'infrastruttura utilizzabile per proiettare la propria influenza fuori dal territorio nazionale o come vettore di attacchi digitali. Esiste un ulteriore scopo che può essere perseguito da parte degli Stati nazionali ed è quello del reindirizzamento delle comunicazioni. In altre parole, i cavi sottomarini possono essere immaginati come delle autostrade sulle quali viaggiano i nostri dati. Come in ogni autostrada esistono dei caselli dove i dati possono prendere altre direzioni che sono rappresentati dai punti di approdo. Pertanto, più sono i punti di approdo che si controllano e maggiore è la mole di dati di cui i paesi possono entrare in possesso. La ridondanza del sistema serve proprio ad evitare questa minaccia. L'unica alternativa al controllo dell'intera autostrada è costringere i dati a passare per i caselli ed i percorsi sotto il proprio controllo. In questo modo sarà possibile non solo ascoltare le conversazioni ma anche decidere se bloccare il traffico di dati o dove veicolarlo. Questo è ciò che si intende quando si parla di "modificare la topologia di Internet"[326]. In questo paragrafo si analizzerà come alcuni paesi autoritari (Cina e Russia) utilizzino le aziende private dei loro cittadini per questo scopo.

Innanzitutto, il 59% dei cavi sottomarini è posseduto da un unico proprietario[327] mentre solo il 19% dei cavi sono posseduti interamente dallo Stato[328]. Il dato è fuorviante in quanto gli stati sono in grado

[326] Op. Cit, J. Sherman, Cyber Defense Across the Ocean Floor, 2021.
[327] Ibidem, pp. 9.
[328] Si precisa che il dato citato fa riferimento alle aziende in cui lo stato risulta l'azionista di maggioranza, direttamente o indirettamente.

di esercitare influenza e pressione nei confronti delle aziende indipendentemente dalla loro quota di partecipazione. Come si vedrà, questo è evidente nei paesi autoritari. In fin dei conti, sono le aziende private che concretamente gestiscono la costruzione ed il monitoraggio dei cavi. La difesa e l'attacco dell'infrastruttura passa necessariamente per queste organizzazioni. Appare evidente che ciò pone delle sfide in termini di sicurezza. Basti pensare che un'azienda che costruisce cavi sottomarini potrebbe essere costretta dal proprio stato ad inserire delle backdoor che ne consentano il monitoraggio dei dati senza che nessuno se ne accorga.

Entity	Ownership by Chinese Government	Number of Sole-owned Cables	Number of Co-owned Cables
China Mobile	State-owned	1	10
China Telecom	State-owned	0	15
China Unicom	State-owned	0	12
CITIC Telecom International	State-controlled	0	1
CTM	State-controlled	0	1
National Grid Corporation of the Philippines	Beijing is a consortium member	0	1

Figura 28: Op. Cit, J. Sherman, Cyber defense across the Ocean Floor, 2021.

Lo stesso governo degli Stati Uniti ha evidenziato il rischio dell'influenza dello Stato cinese su due fronti: la compromissione dei dati attraverso i proprietari dei cavi[329] e la modifica della forma fisica di Internet per instradare più traffico globale attraverso la Cina[330]. Si tratta di attività realizzabili dalle stesse aziende. La postura aggressiva delle aziende cinesi è stata notata anche da altri paesi quali Taiwan secondo cui Pechino vuole "monopolizzare" le comunicazioni nel Pacifico[331]. L'espansionismo cinese è testimoniato anche dalla forte crescita delle aziende cinesi citate in Figura 3. Inoltre, il 36% dei cavi posseduti dalle aziende statali (China Mobile, China Telecom, China Unicom) non hanno punti di approdo in Cina. Questo indica come più di un terzo degli investimenti sono su cavi che non verranno direttamente utilizzati dai cittadini cinesi. In questi casi lo scopo non è quello di aumentare la ridondanza del sistema ma possedere il controllo delle comunicazioni in determinate aree geografiche come analizzato nel paragrafo precedente. D'altro canto, solo se si possiedono le autostrade su cui viaggiano i dati all'estero è possibile reindirizzare il traffico di rete verso i propri confini.

[329] Ad esempio la raccolta di informazioni di intelligence attuata in un punto di approdo controllato dallo Stato
[330] Ad esempio, creando più punti di strozzatura nella rete globale sotto il controllo del governo cinese.
[331] Brennan and Feng, "Taiwan Says China Wants to Spy.", Newsweek, 18 dicembre 2020. Accessibile a https://www.newsweek.com/taiwan-china-spy-nations-steal-data-undersea-cable-networks-kiribati-connectivity-project-1555849.

Non sono solo i proprietari dei cavi a risentire dell'influenza cinese ma anche le aziende che li costruiscono e posano. In questo caso, lo scopo è quello di far inserire delle backdoor durante l'installazione del cavo che permettano allo stato di spiare le conversazioni che vi passano all'interno[332]. Il pericolo è stato sottolineato da numerosi osservatori ma ufficialmente non sono mai state scoperte operazioni di questo tipo[333]. In questo campo Huawei Marine è la principale azienda cinese. Il coinvolgimento della sola società cinese Huawei Marine nello sviluppo di cavi sottomarini in tutto il mondo è quasi raddoppiato in seguito all'annuncio del DSR, con cinque nuovi sistemi tra il 2012 e il 2016 e otto tra il 2015 e il 2019, una tendenza non eguagliata da altri leader del settore. A differenza di aziende di dimensioni simili, la maggior parte dello sviluppo dei cavi di Huawei avviene anche al di fuori della sua regione d'origine a testimonianza di come la strategia cinese sia quella di proiettare la propria influenza in paesi esteri.

4.2 LA RUSSIA

La Russia è stata tra i primi paesi a capire l'importanza dei cavi sottomarini in chiave geopolitica. Già durante la Guerra Fredda, la flotta russa disponeva di un apposito dipartimento per l'intelligence marittima che era responsabile di tutte le operazioni condotte dalle navi per la raccolta di informazioni, comprese operazioni speciali ai danni delle infrastrutture critiche[334]. Nel corso del tempo, questa tattica si è inserita sempre di più nel pensiero strategico russo che, rispetto a quello del periodo sovietico, presentava notevoli differenze. Se la Guerra Fredda si era contraddistinta per una gestione dell'escalation tramite la deterrenza militare (specialmente quella nucleare), dagli anni 90 si afferma una visione maggiormente olistica in cui acquisiscono valore gli strumenti non militari che fanno leva sull'intimidazione della popolazione e dei costi sociali ed economici che potrebbero scaturire da un eventuale conflitto[335]. Pertanto, la capacità di infliggere danni economici è ritenuta una componente essenziale nella gestione di conflitti locali e nello scoraggiare interventi esterni. La marina russa continua a dare la priorità al miglioramento delle proprie capacità per operazioni asimmetriche e ibride marittime e, per la Russia, l'approccio ibrido è preferibile in quanto offre

[332] Op.Cit, J. Sherman, Cyber Defence Across the Ocean Floor, pp. 15.
[333] G. Corera, "Huawei: MPs claim 'clear evidence of collusion' with Chinese Communist Party," BBC News, 8 Ottobre 2020. Accessibile a https://www.bbc.com/news/technology-54455112; Lindsay Maizland and Andrew Chatzky, Huawei: China's Controversial Tech Giant, Council on Foreign Relations, 6 Agosto, 2020. Accessibile a https://www.cfr.org/ backgrounder/huawei-chinas-controversial-tech-giant; Li Tao, "Huawei says relationship with Chinese government 'no different' from any other private company in China," South China Morning Post, December 26, 2019
[334] Berkowitz, Marc J. "Soviet Naval Spetsnaz Forces." *Naval War College Review* 41, no. 2 (1988): 5–21. Accessibile a http://www.jstor.org/stable/44636878.
[335] M. Kofman, A. Fink, J. Edmonds, Russian Strategy for Escalation Management: Evolution of Key Concepts, The Center for Naval Analyses, 13 Aprile 2020, pp.94. Accessibile a https://www.cna.org/reports/2020/04/russian-strategy-for-escalation-management-key-concepts

possibilità di negazione plausibile, implica un basso livello di sensibilità morale e sfrutta anche le aree grigie dell'Art. 5 della NATO[336].

Queste considerazioni sono ben note ai leader militari occidentali che negli ultimi anni hanno denunciato più volte la serietà di queste minacce. Nel 2017, il maresciallo capo dell'aeronautica Sir Stuart Peach, allora capo della difesa britannica, ha ammesso apertamente che la Gran Bretagna e i suoi alleati della NATO erano impreparati ad affrontare uno scenario del genere, citando come prova la crescente attività russa nel GIUK Gap[337] (Groenlandia, Islanda e Stati Uniti e Regno Unito). Si tratta di una regione strategica in quanto ospita cavi sottomarini cruciali la cui interruzione avrebbe un grave impatto sulla comunicazione tra i membri della NATO nell'area. Ad alzare il livello di tensione sono arrivate le parole del capo delle forze armate britanniche, Amm. Tony Radakin, secondo cui qualsiasi tentativo di danneggiare i cavi potrebbe essere considerato un atto di guerra[338]. Il Comitato per la scienza e la tecnologia (STC) della NATO ha evidenziato in un rapporto del 2019 che la Russia possiede una delle capacità di guerra sui fondali marini più avanzate al mondo[339]. Pertanto, la leadership militare della NATO è pienamente consapevole dell'aggressiva esplorazione da parte della marina russa delle reti di cavi di comunicazione sottomarini. Negli ultimi tempi si è registrato un aumento significativo dell'attenzione russa sui cavi sottomarini transatlantici, in particolare quelli nell'Oceano Atlantico settentrionale. È importante notare che l'attività navale russa non si limita ai cavi per comunicazioni commerciali ed infatti vengono presi di mira anche i cavi gestiti dai militari che non sono facilmente visibili sulle mappe normali. Questi sistemi classificati includono l'Integrated Undersea Surveillance System (IUSS), che consiste in sistemi acustici fissi e mobili utilizzati per scopi di rilevamento subacqueo militare come il Sound Surveillance System (SOSUS)[340]. Sebbene lo IUSS abbia perso la sua importanza in seguito al crollo dell'Unione Sovietica, il recente aumento dell'attività dei sottomarini russi ha reso questo sistema ancora una volta rilevante per gli Stati Uniti e la NATO. Gli Stati Uniti hanno già riconosciuto questa minaccia, come ha affermato Bryan Clark della CSBA durante un'audizione della sottocommissione per l'energia marittima e le forze di proiezione[341]. Clark ha affermato che "Vedremo anche l'avvento di

[336] Op. Cit, Policy Exchange, Undersea Cables, 2017.
[337] Laurence Peter, "What Makes Russia's New Spy Ship Yantar special?", BBC News, 3 January 2018. Accessibile a https://www.bbc.com/news/world-europe-42543712.
[338] UK Military Chief Warns of Russian Threat to Vital Undersea Cables", The Guardian, 8 gennaio 2022.
[339] Op. Cit, Rowan Allport, "Fire and Ice - A New Maritime Strategy for NATO's Northern Flank", 2018.
[340] Bryan Clark, "Undersea Cables and the Future of Submarine Competition", Bulletin of the Atomic Scientists 72(4): 1-4, 15 giugno 2016. Accessibile a https://www.researchgate.net/publication/304002644_Undersea_cables_and_the_future_of_submarine_competition
[341] "Game Changers - Undersea Warfare", Subcommittee on Seapower and Projection Forces, Committee on Armed Services House of Representatives, H.A.S.C. No. 114-61, From the U.S. Government Publishing Office, 27 ottobre 2015.

famiglie di sistemi sottomarini, o sistemi di sistemi con battelli subacquei e sistemi senza pilota sia sul fondo del mare che mobili … in cui la capacità di trovare le cose sott'acqua, di installarle o rimuoverle diventa molto importante, e chi può farlo meglio dell'altro concorrente otterrà un vantaggio. Possiamo vederlo anche in questo momento con gli sforzi che i russi stanno facendo per cercare di identificare e localizzare i cavi sottomarini"[342].

4.2.1 Organizzazione interna: l'intelligence dei fondali marini

A differenza dei paesi Occidentali, la Russia possiede una precisa governance per i fondali sottomarini e le attività di intelligence e sabotaggio subacquee a dimostrazione del ruolo strategico che ricopre questo settore per Mosca. Le due principali organizzazioni sono la Marina Russa e la Direzione della Ricerca Subacquea della Marina Russa (GUGI - Glavnoye Upravleniye Glubokovodnykh Issledovaniy) con sede nella baia di Olenya (penisola di Kola). Quest'ultimo è un ente particolare. A livello organizzativo è distaccato dalla Marina e risponde direttamente al Ministero della Difesa e dalla Direzione Generale per le informazioni militari (GRU) ma a livello operativo attira personale dalla 29ª divisione sottomarina separata. Il GUGI dispone di sottomarini specializzati per operazioni in acque profonde come il Paltus, l'X-Ray, il Kashalot ed il Losharik. Come si analizzerà meglio in seguito, ciò che rende unici questi sottomarini è il loro scafo in titanio che gli permette di immergersi fino ai 2500 metri. Il GUGI non è solo responsabile del danneggiamento delle infrastrutture critiche ma possiede altri compiti molto delicati tra cui il posizionamento dei sensori della rete Harmony per il monitoraggio dei movimenti subacquei[343]. Inoltre, una delle navi madre del GUGI, la Belgorod, imbarcherà i siluri nucleari Poseidon con i quali Putin ha minacciato di "spazzare via" la Gran Bretagna[344].

La Direzione Intelligence dello Stato Maggiore della Marina russa è fortemente coinvolta in questo tipo di attività. Dal punto di vista organizzativo essa è subordinata alla quinta Direzione del GRU tanto che da 1977 il direttore dell'intelligence navale russa è stato sempre il Vicedirettore del GRU. Fin dall'epoca sovietica, alla Marina è stato assegnato il compito di tenere i rapporti con i mercantili civili che potevano essere cooptati sia in funzioni di raccolta di informazioni che di sabotaggio. Le unità Spetsnaz controllate dalle flotte regionali possono essere inserite in teatro utilizzando una serie

[342] Ibidem.
[343]Intelligence Online, Acoustic warfare in the Barents Sea, 26 luglio 2023. Accessibile a https://www.intelligenceonline.com/surveillance--interception/2023/07/26/acoustic-warfare-in-the-barents-sea,110007360-art
[344] Sky Tg24, Guerra in Ucraina, Tv Russa: "Con il missile Poseidon tsunami atomico sulla Gran Bretagna", Mondo. Accessibile a https://tg24.sky.it/mondo/2022/05/03/russia-missile-poseidon.

di veicoli e possono essere utilizzate sia per la sorveglianza che per operazioni segrete contro obiettivi militari e civili[345]. Da questo punto di vista, un caso ben noto e recente è quello della distruzione del Gasdotto North Stream 2 che, secondo alcuni analisti, avrebbe coinvolto personale specializzato del GUGI e pescherecci civili[346].

La biforcazione delle responsabilità tra l'intelligence navale, che risponde al GRU, e il GUGI – che apparentemente opera come una direzione all'interno del Ministero della Difesa russo – sembrerebbe creare una divisione artificiale tra risorse che svolgono funzioni simili. Come mai le risorse siano spartite in questo modo e l'esatta differenziazione delle responsabilità non sono elementi semplici da comprendere. Da una parte è probabile che la Marina, sotto il quinto dipartimento del GRU, mantenga compiti maggiormente operativi come il monitoraggio delle risorse navali occidentali mentre il GUGI mantenga il controllo sulle risorse considerate strategiche come le infrastrutture critiche. D'altra parte, il fatto che tali compiti siano stati sottratti alla Marina è riconducibile alla riaffermazione del controllo da parte dello Stato Maggiore russo sulla Marina sovietica sotto il mandato del maresciallo Nikolai Ogarkov e dell'allora ministro della Difesa sovietico Dmitri Ustinov[347].

Come si può evincere dalle risorse militari di cui dispone e dal suo assetto organizzativo, la Russia si muove su un doppio binario: da una parte quello della forza tramite il dispiegamento di sottomarini e droni subacquei e dall'altro vi è l'utilizzo della flotta mercantile nelle zone adiacenti ai cavi sottomarini. Queste due tattiche pongono diverse sfide ai sistemi di sicurezza occidentali. Nel primo caso si tratta di un ritorno ad un contesto da Guerra Fredda in cui la sorveglianza dei sottomarini era uno dei campi di battaglia principali. Sebbene l'Occidente abbia sviluppato importanti sistemi di rilevamento dei sottomarini, si tratta di uno dei settori in cui la Russia possiede un gap tecnologico minore con la NATO. Da questo punto di vista, la vera sfida riguarda le regole di ingaggio. Nelle acque territoriali, i paesi possono perseguire in modo aggressivo i sottomarini stranieri che rilevano, cosa che i sovietici facevano spesso con i sottomarini statunitensi durante la Guerra Fredda, e viceversa. Nelle acque internazionali, tuttavia, è probabile che ciò costituisca una sfida maggiore ed il rischio di incidenti può essere molto alto. Nel secondo caso ci si trova dinnanzi ad un tipico esempio di guerra ibrida in cui l'attribuzione del danno può risultare complicata. Dal punto di vista della normativa internazionale ci sono margini di manovra più ampi per intervenire sui pescherecci

[345] Op. Cit. Berkowitz, Marc J. Soviet Naval Spetsnaz Forces.", 1988.
[346] Andrii Ryzhenko, Nord Stream Explosions: Russian Sabotage in the Baltic?, The Jamestown Foundation, Eurasia Daily Monitor Volume: 19 Issue: 146, 4 ottobre 2022**.** Accessibile a https://jamestown.org/program/nord-stream-explosions-russian-sabotage-in-the-baltic/
[347] Dr. Sidharth Kaushal, Stalking the Seabed: How Russia Targets Critical Undersea Infrastructure, Royal United Services Institute 25 maggio 2023. Accessibile a https://rusi.org/explore-our-research/publications/commentary/stalking-seabed-how-russia-targets-critical-undersea-infrastructure.

sospettati di danneggiare cavi sottomarini come previsto dalla Convenzione sui cavi del 1884 che permette alle marine di abbordare queste navi. Allo stesso modo, la Convenzione delle Nazioni Unite sul diritto del mare (UNCLOS) consente ai paesi di limitare le attività delle navi civili che conducono sorveglianza rilevante per lo sfruttamento economico all'interno delle loro zone economiche esclusive (ZEE). In questo caso, la difficoltà è relativa all'individuazione e classificazione di queste imbarcazioni come "pericolose" in modo analogo a quanto avviene nelle attività di polizia per la lotta al contrabbando e alla pirateria. E' necessario che una nave sospetta venga identificata in mezzo a un gran numero di navi che conducono una normale attività economica. Per far fronte a queste minacce sono necessarie nuove forme di collaborazione sia con i partner privati che gestiscono queste infrastrutture e che sono sempre più presenti nei fondali marini sia a livello nazionale tramite accordi quadro a livello regionale che permettano una più stretta forma di coordinazione tra i singoli stati, specialmente nella regione baltica.

Allo stesso modo, l'integrità delle infrastrutture critiche è una preoccupazione strategica per la Russia. Nel decreto presidenziale del 2016 "Sull'approvazione della dottrina della sicurezza informatica della Russia", la dipendenza da sistemi di comunicazione stranieri viene considerata una potenziale minaccia[348]. Ciò, afferma il decreto, è il risultato del potenziale spionaggio da parte di potenze straniere di dati appartenenti alla Russia e ai suoi cittadini attraverso lo sfruttamento di infrastrutture informative. Inoltre, il fatto che la proprietà e il controllo dei cavi sottomarini siano distribuiti in modo sproporzionato tra stati considerati ostili alla Russia è considerato una minaccia geopolitica per lo stato, poiché l'accesso a tali infrastrutture potrebbe essere intenzionalmente limitato dagli avversari occidentali in caso di conflitto[349]. Queste preoccupazioni hanno portato a diversi test su scala nazionale rispetto alla resilienza del sistema Runet[350] in caso di un attacco ai cavi sottomarini[351]. Il tentativo della Russia di "scollegarsi" da internet è da leggere in chiave difensiva rispetto a possibili

[348] Prezident Rossiiskoi Federatsii, "Ob utverzhdenii doktriniy informatsionnoy bezopasnosti Rossiiskoi Federatsii", Administratsiya Prezidenta Rossii, pubblicato il 5 dicembre 2016 Accessibile a http://static.kremlin.ru/media/acts/files/0001201612060002.pdf

[349] J. Katzman, Securitization of Physical Cyberspace Infrastructure as a Nexus in U.S.-Russia Relations: The Case of Submarine Communications Cables, Russian International Affairs Council, 18 febbraio 2022. Accessibile a https://russiancouncil.ru/en/analytics-and-comments/columns/cybercolumn/securitization-of-physical-cyberspace-infrastructure-as-a-nexus-in-u-s-russia-relations-the-case-of/

[350] Consiste in una struttura internet interna alla Russia alla quale possono accedere solamente i residenti nel paese e che dovrebbe permettere alla Russia di isolarsi dall'internet globale.

[351] Alexandra Brzozowski , NATO seeks ways of protecting undersea cables from Russian attacks, Euractiv, 23 ottobre 2020.
Accessibile a https://www.euractiv.com/section/defence-and-security/news/nato-seeks-ways-of-protecting-undersea-cables-from-russian-attacks/

attacchi cyber nei suoi confronti. Tuttavia, una decisione di questo tipo comporterebbe diversi problemi come, ad esempio, la totale esclusione dalle transazioni finanziarie.

A conferma di quanto detto, in un incontro dell'agosto 2020, il presidente di Rostelecom Mikhail Oseyevsky ha dichiarato al presidente russo Vladimir Putin che l'azienda stava "completando un ambizioso programma di espansione delle infrastrutture di base in Estremo Oriente", avendo recentemente posato i cavi fino alle isole russe. Oseyevsky ha aggiunto che Rostelecom vede "ulteriori opportunità di lavoro sui mercati internazionali" alla luce dei crescenti volumi globali di traffico Internet, una situazione in cui "la Russia può fornire il metodo più semplice e affidabile per trasmettere questi volumi dall'Europa all'Asia"[352]. Questo è significativo perché Rostelecom è un'azienda di proprietà dello Stato e tutti gli "incontri" di questo tipo con Putin sono programmati. Quindi, oltre alle probabili dimensioni di sicurezza della conquista dell'infrastruttura Internet da parte della Russia, sembra avere anche dimensioni economiche, con i cavi sottomarini che servono al Cremlino come potenziale meccanismo per aumentare le sue leve di coercizione economica[353].

4.2.2 Gli assetti della Marina Militare Russa

La Russia dispone di una flotta dedicata alle operazioni subacquee tra le più avanzate del mondo per via dei forti investimenti che hanno coinvolto la sua Marina nel corso dell'ultimo decennio. La sua capacità operativa può raggiungere i 5000 metri grazie a diversi dispositivi di cui dispone tra cui i sottomarini madre che schierano minisommergibili a propulsione nucleare per immersioni profonde, la nave dell'intelligence Yantar che supporta Remotely Operated Vehicle (ROV) e minisommergibili con equipaggio, diverse tipologie di Unmanned Underwater Vehicles (UUV) ed infine dei sommergibili dual-use con equipaggio che possono lavorare anche su cavi tramite appositi bracci robotici[354].

[352] Kremlin.ru, "Meeting with Rostelecom President Mikhail Oseyevsky," 5 agosto 2020, Accessibile a http://en.kremlin.ru/events/president/news/63857
[353] Op. Cit, J. Sherman, Cyber Defense Across the Ocean Floor, 2021.
[354] H I Sutton, "5 Ways The Russian Navy Could Target Undersea Internet Cables", Naval News, 7 Aprile 2021. Accessibile a https://www.navalnews.com/naval-news/2021/04/5-ways-the-russian-navy-could-target-undersea-internet-cables/

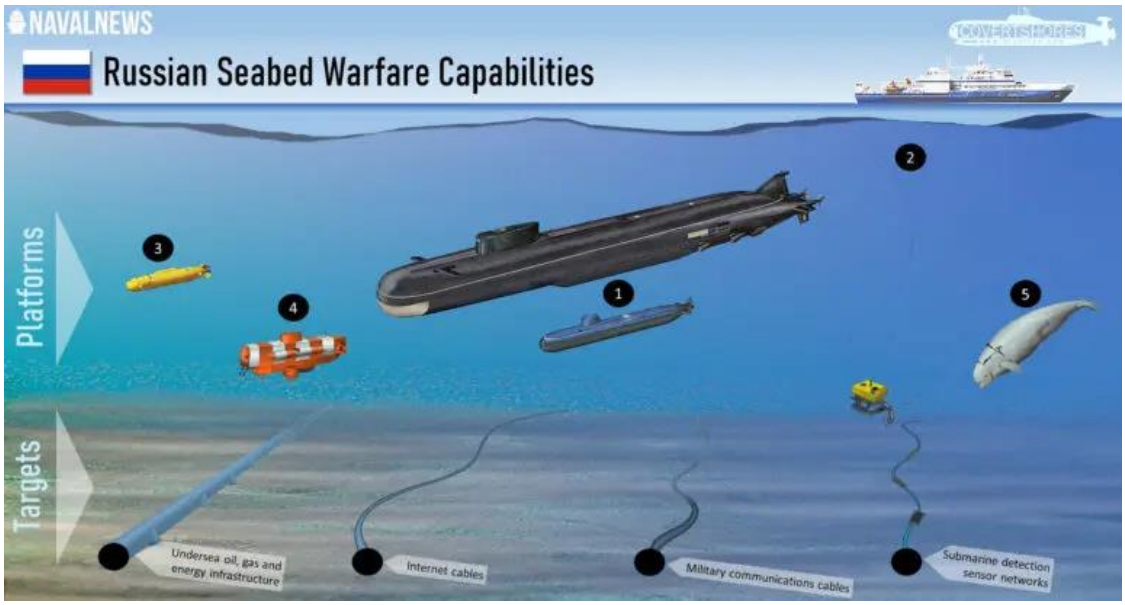


Figura 29: A. Lucas Da Silva, The importance of protecting submarine cables in an interconnected world, ofcs.report, 6 aprile 2023.

Sebbene siano a propulsione nucleare, i mini-sottomarini sono relativamente piccoli, il che rende difficile il sostentamento degli equipaggi per lunghi periodi. Pertanto, hanno bisogno di essere supportati dalle navi madre nei viaggi più lunghi. Per questo ruolo, i sovietici e poi la Federazione Russa hanno tipicamente utilizzato versioni allungate dei sottomarini con missili balistici a propulsione nucleare (SSBN) in pensione come la classe *Yankee* e dei sottomarini con missili da crociera a propulsione nucleare (SSGN) come la classe *Oscar*. Le due attuali navi madre del GUGI sono la K-329 *Belgorod*, la *BS-64 Podmoskovye* e la BS-136 Orenburg[355]. Il Belgorod è la conversione di una classe Oscar II. È lungo 178 metri, largo 15 metri e con un dislocamento di 19.000 tonnellate[356]. Entrato in servizio nel 2019 si presta sia come nave madre per il minisottomarino Losharik per svolgere operazioni speciali[357] e sia per la deterrenza nucleare imbarcando sei siluri Poseidon (2M39 o Status-6), lunghi 20 metri con propulsione nucleare e testata da 100 megaton. Il BS- Podmoskovye è un battello lanciamissili balistici (ex classe Delta IV) i cui lavori sono stati completati nel 2012. Le modifiche che ha subito allo scafo gli permettono di operare come nave madre del mini-sottomarino Losharik.

Questi sottomarini possono operare per lunghi periodi di tempo nelle profondità marine, per operazioni di salvataggio, di ricerca scientifica, per il posizionamento di strumentazione di ascolto di comunicazioni sui cavi sottomarini e in operazioni di sabotaggio dei cavi. Gli stessi, inoltre, svolgono

[355] Rowan Allport, "Fire and Ice - A New Maritime Strategy for NATO's Northern Flank", Human Security Centre, 3 Dicembre 2018.
[356] H I Sutton, "Russia's Gigantic Submarine, Belgorod, Sails For The First Time", Naval News, 25 gugno 2021.
[357] Caleb Larson, "Belgorod: Russia's Stealth Submarine Has the Navy Really Confused", The National Interest, 26 luglio 2021.

operazioni per il posizionamento di sensori subacquei idroacustici per il monitoraggio dei sottomarini della NATO (similare al sistema SOSUS statunitense) e di generatori nucleari autonomi (ATGU - Autonomous Nuclear Turbine Generator), per la distribuzione di energia elettrica per la perforazione petrolifera in mare, per i sensori subacquei e altre strutture sottomarine. Ad oggi, nessuno di questi sottomarini ha operato nel Mediterraneo ma solamente nell'area Artica e dell'Oceano Atlantico[358]. Ai due battelli madre si aggiungono diversi minisottomarini a propulsione nucleare; 2 Paltus (Project 18511) che sono impiegati per attività di disturbo dei sottomarini, attività di intelligence subacquea e sollevamento di oggetti dal fondo del mare[359]. Il Losharik (NORSUB-5) è in realtà una stazione di ricerca nucleare in acque profonde. Possiede delle caratteristiche tecniche uniche: è lungo 74 metri e possiede un doppio scafo in titanio la cui parte interna è costituita da sette sfere unite tra loro che ospitano un equipaggio di 25 uomini. Grazie a queste caratteristiche il Losharik può operare per lunghi periodi di tempo ad elevate profondità, si dice fino a 6.000 metri[360]. Tuttavia, il Losharik ha subito un grave incidente il 1° luglio 2019, quando un incendio nel vano batteria ha ucciso 14 membri dell'equipaggio e, risulta ancora in riparazione. Ai battelli subacquei si è aggiunta la nave da ricerca Yantar classificata come Auxiliary General Oceanographic Research (AGOR) ma, nota anche come "Oceanographic Research Vessels" (ORV) and "Search-and-Rescue Vessels" (SRV). La nave, lunga 108 m, larga 17 m e con un dislocamento di 5200 t è entrata in servizio nel 2015 come capoclasse del Project 22010[361]. Trasporta due Manned Underwater Vehicles (MUV) di classe Rus e Konsul in grado di immergersi fino a 6.000 metri per 10-12 ore alla volta, minisommergibile con equipaggio ARS-600, che può operare fino a 1000 metri di profondità oltre a Remote Operated Vehicle (ROV) che possono svolgere un'ampia gamma di attività subacquee[362].

[358] A. Masiello, Sicurezza delle reti e infrastrutture critiche nel Mediterraneo, Italia Strategic Governance, Dicembre 2022, pp.5. Accessibile a https://aliseoeditoriale.it/wp-content/uploads/2022/12/Sicurezza-reti-e-infrastrutture-critiche-nel-Mediterraneo.pdf
[359] The Threat to World's Communications Backbone – The Vulnerability of Undersea Cables", Navy Lookout, 10 marzo 2021.
[360] Op. Cit, A. Masiello, Sicurezza delle reti e infrastrutture critiche nel Mediterraneo, 2022.
[361] Martin Manaranche, "Yantar Shipyard Services "Oceanographic Research Vessel" Yantar", Naval News, 27 maggio 2020.
[362] Saverio Lesti, Seabed Warfare: la Minaccia Asimmetrica alle Comunicazioni Globali, Mondo Internazionale (Focus – Allegati), 23 marzo 2022.

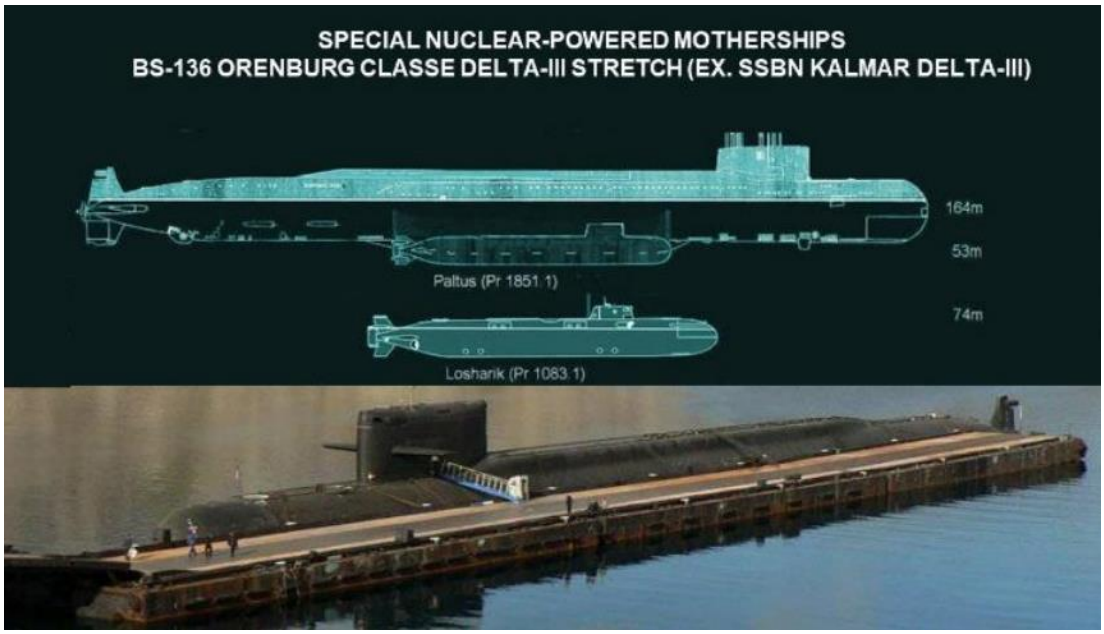


Figura 30: Figura 7: A. Masiello, La sicurezza delle reti e delle infrastrutture critiche nel Mediterraneo, Italia Strategic Governance, dicembre 2022, pp.6.

Le operazioni della Yantar nel Mediterraneo risalgono al 2016 anno in cui sarebbe stata avvistata in zone adiacenti ai cavi sottomarini TURCYOS-2, UGARIT (con punti di atterraggio a Cipro e in Siria) e I-ME-WE che collega Marsiglia a Mumbai. Formalmente era impegnata in operazioni di mappatura ma è possibile che il suo scopo fosse quello di posizionare dispositivi di ascolto per intercettazioni sui cavi. La Yantar sembra essere assente dal Mare Nostrum da diverso tempo ma ciò non vuol dire che altre navi mercantili o scientifiche non possano aver ricoperto la medesima funzione. Ne sono un esempio la nave di ricerca scientifica ADMIRAL VLADIMIRSKY, che tra novembre e dicembre 2022 ha operato nel Mar del Nord lungo la costa orientale della Gran Bretagna e nel Mar Baltico e la nave di ricerca oceanografica AKADEMIK IOFFE, che il 29 novembre 2022 è entrata nel Mediterraneo attraverso lo stretto di Gibilterra con direttrice stretti turchi e Mar Nero.

Ulteriore tecnica impiegata dalla Marina russa per le attività di ricognizione sottomarina è quella dell'utilizzo di cetacei che, dotati di imbracatura con fotocamera, svolgerebbero ricognizione dei fondali marini fino ad una profondità di 1000 metri[363]. Dalla fine del 2018, una unità cetacei denominata "Combat Dolphin" sarebbe presente nel Mediterraneo orientale, nella base navale russa di Tartus (Siria).

[363] Op. Cit, A. Masiello, Sicurezza delle reti e infrastrutture critiche nel Mediterraneo, 2022.

4.2.3 I Cavi Sottomarini Danneggiati in Norvegia

Nell'aprile 2021 il Lofoten-Vesterålen Ocean Observatory (LoVe), attivo dall'agosto del 2020 e gestito dal Institute of Marine Research (IMR), subisce un malfunzionamento[364]. L'infrastruttura, oltre a raccogliere dati oceanografici, permette anche di raccogliere informazioni e dati sull'attività navale subacquea a vantaggio del Norwegian Defense Research Establishment (FFI) che analizza in anticipo i dati raccolti in modo da eliminare eventuali informazioni riguardanti attività militari[365]. Secondo le indagini, sarebbero stati recisi il "Nodo 2" ed il "Nodo 3" facendo scomparire 4 km di cavi. Ciò che ha destato particolare sospetto è il fatto che dalle ricerche dei dati satellitari non risulta la presenza di imbarcazioni nei momenti dei problemi al sistema[366]. Senza dimenticare che se un peschereccio avesse accidentalmente tagliato il cavo, lo avrebbe prontamente segnalato. Tutti gli indizi fanno pensare ad una nave con il trasponder spento e quindi ad una potenza straniera. Secondo il sito specializzato The Drive vi potrebbero essere diverse ragioni per attuare una simile operazione[367]: in primis il LoVe è uno strumento importante per la Norvegia per tracciare l'attività dei sottomarini stranieri nel Mare di Norvegia limitando potenzialmente alcune operazioni in queste acque; secondariamente la potenza straniera potrebbe aver voluto studiare le informazioni che il sistema è in grado di raccogliere ed infine i cavi stessi possono fornire preziose informazioni tecniche.

All'inizio del 2022, la Space Norwegian Company ha annunciato un'interruzione del sistema di cavi sottomarini delle Svalbard. Questa interruzione è avvenuta tra i 130 e 230 chilometri da Longyearbyen, in una zona dove il fondale marino passa da 300 metri a 2700 metri nel Mar di Groenlandia. I cavi, che collegano Longyearbyen con la Norvegia settentrionale, sono fondamentali per fornire Internet a banda larga e supportare il complesso SvalSat, dotato di oltre 100 antenne satellitari che aiutano nel funzionamento dei satelliti in orbita polare. Questi cavi, lunghi rispettivamente 1.375 e 1.339 chilometri, sono stati progettati in modo ridondante per garantire una connettività ininterrotta. Tuttavia, il guasto di un cavo ha comportato la perdita di questa ridondanza, ponendo una potenziale minaccia di isolamento di Longyearbyen e SvalSat dal resto del mondo. L'importanza di questo incidente è ulteriormente sottolineata dal fatto che la polizia norvegese ha espresso la convinzione che il danno al cavo sia stato probabilmente causato dall'attività umana.

---

[364] Thomas Newdick, "Norwegian Undersea Surveillance Network Had Its Cables Mysteriously Cut", The War Zone, 11 November 2021. Accessibile a https://blog.geogarage.com/2021/11/norwegian-undersea-surveillance-network.html

[365] Op. Cit,Saverio Lesti, Seabed Warfare: la Minaccia Asimmetrica alle Comunicazioni Globali, marzo 2022.

[366] Gabriel Carrer, Rete di cavi sottomarini va ko in Norvegia. Una pista porta a Mosca, Formiche.net, 15 novembre 2021. Accessibile a https://formiche.net/2021/11/norvegia-rete-di-cavi-sottomarini-ko-pista-russa/.

[367] T. Newdick, Norwegian Undersea Surveillance Network Had Its Cables Mysteriously Cut, The Drive, 11 novembre 2021.
Accessibile a https://www.twz.com/43094/norwegian-undersea-surveillance-network-had-its-cables-mysteriously-cut

4.3 STATI UNITI

Come dice Dario Fabbri, "Internet è un fenomeno profondamente americano, soggetto all'interesse geopolitico della superpotenza, in coincidenza con il suo dominio planetario. Nella versione attuale, è stato sviluppato da privati, ma è nato nel grembo militare degli Stati Uniti ed è ancora funzionale alle esigenze strategiche del paese"[368]. In tal senso, la difesa dei cavi sottomarini è cruciale per gli interessi strategici degli Stati Uniti. Il sabotaggio e lo spionaggio di questa infrastruttura possono compromettere la sicurezza nazionale oltre ad apportare dei danni economici difficilmente calcolabili. Negli ultimi anni è cresciuta vertiginosamente l'attenzione nei confronti dell'attività di spionaggio cinese che sembrerebbe aver preso di mira numerosi ufficiali americani[369]. Nel rapporto annuale dell'Intelligence statunitense viene specificato che "La Cina può lanciare attacchi informatici che, come minimo, possono causare interruzioni temporanee e localizzate alle infrastrutture critiche negli Stati Uniti"[370]. Ad oggi, non vi è un documento che indichi la strategia degli Stati Uniti in materia e ciò si deve alla mancanza di una governance chiara che possa indicare la strada da perseguire. Pertanto, si susseguono diversi approcci che riflettono le proposte delle diverse agenzie ed esecutivi.

4.3.1 Il quadro giuridico degli stati uniti e le sue risposte politiche

Il framework legislativo degli Stati Uniti presenta diverse criticità. In primis, la governance dei cavi sottomarini risulta particolarmente frammentaria con il risultato che vi siano molte leggi e regolamenti emanati da enti diversi e incoerenti tra loro. A livello governativo, i cavi sottomarini sono stati designati come "Infrastruttura critica" ma da ciò non sono conseguite politiche di protezione o particolari standard tecnici[371]. Questo sarebbe un compito della Cybersecurity and Infrastructure Security Agency (CISA), tuttavia da un audit del Dipartimento per la Sicurezza Nazionale è emerso come il CISA abbia incontrato numerose difficoltà nell'esercizio del suo ruolo per via delle poche aziende che hanno aderito al programma di condivisione delle informazioni[372]. Ciò ha fatto sì che non si riuscissero a creare degli standard tecnici per i cavi sottomarini. Queste

[368] D. Fabbri, *L'impero informatico americano alla prova cinese*, Limes – "La Rete a Stelle e Strisce", Settembre 2018.
[369] J. Bateman, U.S – China Technological "Decoupling", Capitolo "Limiting Chinese National Security Espionage", Carnegie, 2022, pp.65.
[370] "Annual Threat Assessment of the US Intelligence Community," Director of National Intelligence, 9 aprile 2021, Accessibile a https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf.
[371] Secondo il Gruppo di Lavoro per le infrastrutture critiche, "Nessuna agenzia federale ha recepito la decisione di considerare i cavi come infrastrutture critiche in termini pratici per adottare o applicare standard o politiche di sicurezza". Vedi The Communications Sec., Reliability and interoperability Council IV, Working Group 8, Submarine Cable Routing and Landing, 1 Dicembre 2014. Accessibile a https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG8_Report1_3Dec2014.pdf.
[372] Joseph Cuffati, DHS Made Limited Progress to Improve Information Sharing under the Cybersecurity Act in Calendar Years 2017 and 2018, Office Inspector General, 25 settembre 2020. , Accessibile a DHS Made Limited Progress to Improve Information Sharing under the Cybersecurity Act in Calendar Years 2017 and 2018.

problematiche sono accentuate dall'opposizione delle associazioni di categoria, come la North American Submarine Cable Association (NASCA), a cedere potere agli enti pubblici. La National Oceanic and Atmosperich Administration (NOAA), che è una delle tante agenzie coinvolte a vario titolo nella regolamentazione dei cavi sottomarini, ha sottolineato come "diverse agenzie statunitensi hanno l'autorità di regolamentare la posa e la manutenzione dei cavi al largo delle coste"[373]. Ad esempio, la stessa NOAA ha il compito di "regolamentare se e come i cavi sottomarini possono essere installati nelle aree marine protette"[374] in quanto è responsabile della gestione e protezione dell'ecosistema marittimo e delle sue risorse[375].

I soggetti che hanno il ruolo principale nell'ambito dell'approvazione di cavi sottomarini sono la Federal Communications Commission ed il U.S Army Corps of Engineers che è disposto sotto il Dipartimento della Difesa. La FCC è il primo ente incaricato di indagare sulla natura dei soggetti che fanno richiesta di approdo di cavi sottomarini negli Stati Uniti. La FCC richiede che vengano fornite informazioni sui soggetti che possiedono o controllano la stazione di approdo via cavo statunitense e le entità che possiedono o controllano una quota pari o superiore al 5% del sistema via cavo[376]. Quando il cavo è controllato almeno per il 10% da un'azienda estera, la FCC si avvale del supporto della "Committee for the Assessment of Foreign Participation in in the United States Telecommunications Services Sector"[377] (nota come Team Telecom) che è composta da membri del Dipartimento per la Sicurezza Nazionale (DHS), Dipartimento della Difesa (DOD) e Dipartimento della Giustizia (DOJ) e può approvare, negare o subordinare la costruzione di un cavo a determinate condizioni[378]. Questi processi possono durare anche diversi anni come avvenuto nel 2019 quando, per la prima volta, il Team Telecom ha negato a China Mobile la costruzione di un cavo dopo otto anni di consultazioni[379]. L'altra licenza che deve sempre essere ottenuta per costruire un cavo sottomarini in acque statunitensi è quella concessa dal U.S Army Corps of Engineers. Esso ha il compito di valutare l'impatto del cavo sulla navigazione ed in generale ha la giurisdizione del fondale

[373] NOAA Office of General Counsel, Submarine Cables—Domestic Regulation, NOAA, 8 Luglio 2019, Accessibile a https://www.gc.noaa.gov/gcil_submarine_cables_domestic.html.
[374] Ibidem.
[375] Op, Cit, Protection of Undersea Telecommunication Cables: Issues for Congress, 2023.
[376] Op, Cit, Protection of Undersea Telecommunication Cables: Issues for Congress, 2023, pp. 15.
[377] E' stata istituita tramite Ordine Esecutivo del Presidente, "Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector," 85 Federal Register 19643-19650, 4 aprile 2020.
[378] Questo processo di approvazione è disciplinato da due fonti principali: il Cable LANDING License Act del 1921 ed il Communications Act del 1934 (sezione 214). Vedi W. Lori, Gordon e Karen L. Jones, Global Communications Infrastructure: Undersea and Beyond, The Aerospace Corporation, Center for space and policy strategy, febbraio 2022, pp. 10.
[379] "FCC Streamlining & Formalizing Team Telecom," National Law Review, October 20, 2020

marino sulla piattaforma continentale esterna[380]. Pertanto, qualsiasi attività che viene svolta in queste aree richiede l'approvazione del USACE. Funzione analoga è svolta anche dal Dipartimento degli interni andando a creare non poca confusione.

Oltre le agenzie federali che possiedono la maggior parte dei poteri regolamentari, vi sono anche le autorizzazioni dei singoli stati. Queste possono riguardare soprattutto le modalità di posa dei cavi sottomarini entro le tre miglia nautiche. Ad esempio, stati come la Florida e l'Oregon richiedono che il cavo venga installato sotto la superficie del fondale e ne verificano l'esecuzione. Ciò può allungare notevolmente i tempi o addirittura bloccare un cavo per cui è stata già ottenuta l'approvazione a livello federale.

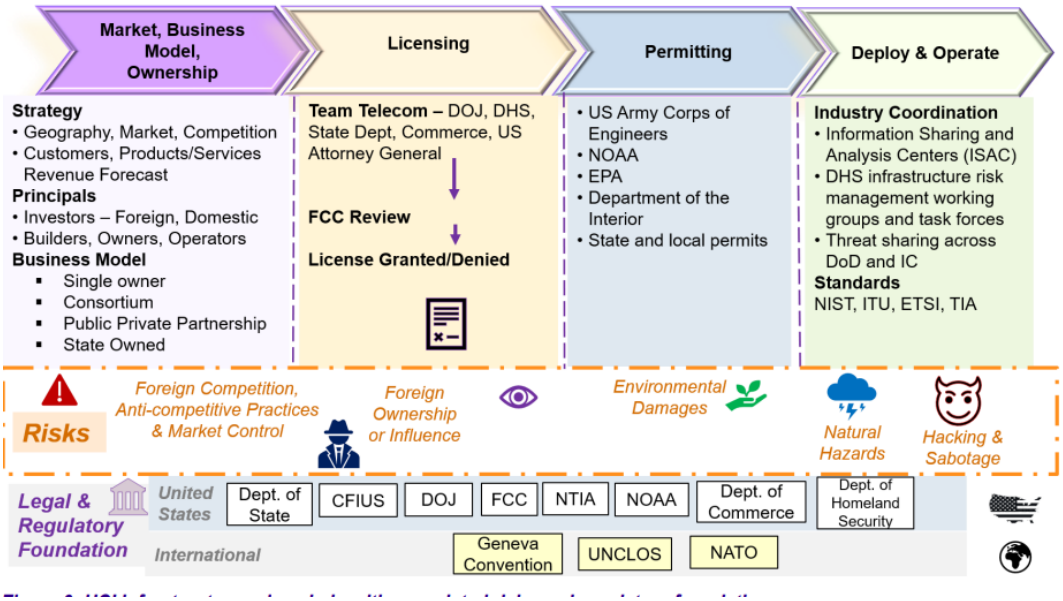


Figura 31:Figura 6: Lori. W. Gordon, Karen L. Jones, Global Communications Infrastructure: Undersea and Beyond, Aereospace Corporation, febbraio 2022, pp.14.

Il Communications Security, and Interoperability Council (CSRIC) ha osservato come "come la vicinanza ad altre attività marine, ai processi di autorizzazione governativa e al raggruppamento dei percorsi e degli approdi dei cavi di approdo possono aumentare il rischio di danni ai cavi e compromettere la resilienza della rete statunitense"[381]. Lo stesso gruppo di lavoro ha sottolineato che nessuno stato abbia legiferato delle distanze minime tra le rotte di cavi sottomarini. Ciò testimonia come la mancanza di collaborazione tra le agenzie comporti un aumento dei rischi in quanto non vi è

[380] Per limite esterno si intende "tutte le terre sommerse che si trovano in mare e al di fuori dell'area delle terre sottostanti le acque navigabili e di cui il sottosuolo e il fondale marino appartengono agli Stati Uniti e sono soggetti alla loro giurisdizione e al loro controllo. Vedi Bureau of Ocean Energu Management, Outer Continental Shelf. Accessibile a https://www.boem.gov/oil-gas-energy/leasing/outer-continental-shelf

[381] CSRIC IV, Working Group 8, Submarine Cable Routing and Landing, Final Report—Protection of Submarine Cables through Spatial Separation, December 2014, pp. 14-15.

un coordinamento nella costruzione di cavi sottomarini ed altre installazioni marittime all'interno di una stessa area.

Tuttavia, anche se il Senato americano ratificasse l'UNCLOS e il Congresso adottasse la legislazione che implementa gli articoli UNCLOS relativi alla protezione dei cavi sottomarini, gli Stati Uniti non avrebbero i mezzi per applicare efficacemente tali articoli[382]. A differenza di paesi come la Nuova Zelanda, ci sono semplicemente troppi cavi lungo la costa degli Stati Uniti per poterli controllare tutti quanti in modo efficace. L'attuale premier britannico Sunak aveva proposto che venissero individuate delle zone protette particolarmente ristrette intorno ai cavi ritenuti più rilevanti[383]. Se da una parte ciò agevolerebbe il monitoraggio dei cavi, dall'altra si porrebbe una questione di legittimità sulla scelta di proteggere maggiormente dei cavi rispetto ad altri. Inoltre, gli Stati Uniti dovrebbero approvare una legislazione che imponga che tutti i cavi sottomarini che attraversano i fondali marini federali siano "cavi oscuri"[384]. Questa idea farebbe sì che solo i proprietari privati e i funzionari pubblici conoscano la posizione del cavo sottomarino rendendo più difficili le operazioni di sabotaggio. Inoltre, gli Stati Uniti devono necessariamente aggiornare le sanzioni relative al danneggiamento di un cavo sottomarino che ad oggi ammontano a 5.000 dollari sulla base di una legge risalente al 1888[385]. Infine, gli Stati Uniti devono centralizzare il monitoraggio dei cavi sottomarini sotto un'unica agenzia. Attualmente, l'agenzia responsabile di tale monitoraggio dipende dallo status giuridico del fondale marino in questione: il risultato è confuso e poco pratico. Ad esempio, la National Oceanic and Atmospheric Administration esercita l'autorità sui cavi posati nei santuari marini nazionali, mentre la Federal Energy Regulatory Commission ha tale autorità per quanto riguarda i cavi posati sulla piattaforma continentale. La razionalizzazione del sistema può essere una parte della soluzione ma è necessario anche assegnare all'FCC un maggiore potere esecutivo e fornire dei fondi adeguati alla sua funzione specialmente per consentirle di verificare che le condizioni che impone ai proprietari dei cavi sottomarini siano effettivamente realizzate.

4.3.2 La guerra fredda dei cavi sottomarini tra Stati Uniti e Cina

Per molti anni non si sono osservati grandi cambiamenti nello scacchiere geopolitico dei cavi sottomarini. L'egemonia novecentesca della Gran Bretagna era stata ereditata dagli Stati Uniti già

[382] K.Frazier, On Protecting the Undersea Cable System, Lawfare, 12 gennaio 2023. Accessibile a https://www.lawfaremedia.org/article/protecting-undersea-cable-system.
Accessibile a https://www.lawfaremedia.org/article/protecting-undersea-cable-system.
[383] Op. Cit, Sunak, Undersea Cables, 2017.
[384]Rack Solutions Blog, What is Dark Fiber and How Does It Work, 18 novembre 2022.
Accessibile a https://www.racksolutions.eu/news/blog/what-is-dark-fiber-and-how-does-it-work/#:~:text=Dark%20fiber%2C%20also%20known%20as,for%20telecom%20and%20network%20communications.
[385] 47 USC Ch. 21, Submarine Cable Act, 29 Febbraio 1888. Accessibile a https://uscode.house.gov/view.xhtml?path=/prelim@title47/chapter2&edition=prelim .

nella seconda metà di secolo. Ad oggi, i cavi sottomarini si estendono per 1,4 milioni di km e sono realizzati ed installati da aziende che principalmente provengono dagli Stati Uniti (SubCom), la Francia (Alcatel Submarine Networks) ed il Giappone (Nec Corp)[386]. Tuttavia, negli ultimi dieci anni il mercato è stato rivoluzionato dall'ingresso delle aziende cinesi che hanno acquisito una percentuale di penetrazione sempre più alta. Questa crescita ha portato HMN Technologies a fornire apparecchiature per il 10% dei cavi sottomarini. Si tratta di una percentuale che sarebbe potuta essere molto più alta se non vi fosse stato l'intervento degli Stati Uniti, preoccupati dall'avanzata cinese in un settore cruciale come questo. Contemporaneamente si è assistito all'ingresso degli OTT (Over the Top) che sono arrivati a possedere il 53% della lunghezza complessiva dei cavi. I colossi tecnologici statunitensi, tra cui Google, Meta e Microsoft, hanno investito circa 2 miliardi di dollari in cavi tra il 2016 e il 2022, pari al 15% del totale mondiale. Nei prossimi tre anni aggiungeranno altri 3,9 miliardi di dollari, ovvero il 35% del totale[387]. Secondo TeleGeography, rappresentano i due terzi dell'utilizzo della larghezza di banda[388]. Si tratta di due dinamiche solo apparentemente distinte. Negli ultimi anni, aziende cinesi e della Silicon Valley si sono trovate a lavorare congiuntamente in più progetti, alcuni dei quali di particolare rilievo per gli Stati Uniti. Nel 2018, Amazon, Meta e China Mobile hanno deciso di lavorare insieme su un cavo che collega la California a Singapore, Malesia e Hong Kong. In seguito, una serie di manovre introdotte da Washington ha portato China Mobile a ritirarsi dal consorzio[389]. Questa sarebbe stata la sesta operazione in quattro anni con cui la Casa Bianca ha impedito la collaborazione tra le sue aziende e quelle di Pechino con lo scopo di proteggere le sue infrastrutture da possibili interferenze.

La prima vittima di questa nuova strategia statunitense è stata Huawei Marine Networks che era entrata nel mercato nel 2008 tramite la costruzione di cavi regionali nel sud est asiatico. L'azienda nasceva come una joint venture con l'inglese Global Marine e già nel 2019 era riuscita a conquistare il 15% del mercato globale attirando le attenzioni della Casa Bianca. Nel 2019, l'amministrazione Trump ha imposto sanzioni a Huawei e al gruppo di telecomunicazioni che ha rapidamente disinvestito dalla joint venture sui cavi sottomarini[390]. Un produttore di cavi regionale cinese poco conosciuto e che per diversi anni ha fornito materiale per l'esercito cinese, Hengtong Group, ha acquistato Huawei Marine e l'ha ribattezzata HMN Tech. Oltre che tramite le sanzioni, la Casa Bianca

[386] Anna Gross, Alexandra Heal, Chris Campbell et al. "How the US is pushing China out of the internet's plumbing", Financial Times, 13 giugno 2023. Accessibile **a https://ig.ft.com/subsea-cables/.**
[387] Ibidem.
[388] R. Cernatoni, The Geopolitics of Submarine Cables, the Infrastructure of the Digital Age, ISPI, 22 giugno 2022. Accessibile a https://www.ispionline.it/en/publication/geopolitics-submarine-cables-infrastructure-digital-age-35516.
[389] Ibidem.
[390] Fibre Systems, Hengtong Optic-Electric to acquire Huawei Marine Networks, 2020**.** Accessibile a https://www.fibre-systems.com/news/hengtong-optic-electric-acquire-huawei-marine-networks.

si è attivata anche informalmente tramite pressioni nei confronti delle aziende terze. Basti pensare a come HMN Tech si sia vista sottrarre il contratto per la realizzazione del cavo da 20.000 km SeaMeWe-6 per un costo di 600 milioni di dollari. Secondo Reuters, per convincere gli investitori a preferire SubCom, l'Agenzia statunitense per il commercio e lo sviluppo (Ustda) avrebbe offerto sovvenzioni per la formazione, per un valore complessivo di 3,8 milioni di dollari, a cinque società di telecomunicazioni dei Paesi che si trovano sul percorso del cavo. A ciò si aggiunga che la diplomazia americana si sarebbe fortemente spesa con le altre aziende sottolineando il rapporto di HMN con l'esercito cinese.

Oggi, solo un cavo fornito da HMN Tech dovrebbe essere operativo in ciascuno degli anni 2024 e 2025, ciascuno dei quali collegherà la Cina esclusivamente ai paesi del sud-est asiatico. Joe Biden ha proseguito con la politica del predecessore in questo ambito, isolando sempre di più i settori high-tech cinesi e portando avanti la filosofia commerciale del *reshoring*: riportare negli Usa le produzioni tecnologiche più d'avanguardia e tenere l'innovazione fuori dalla portata di Pechino[391].

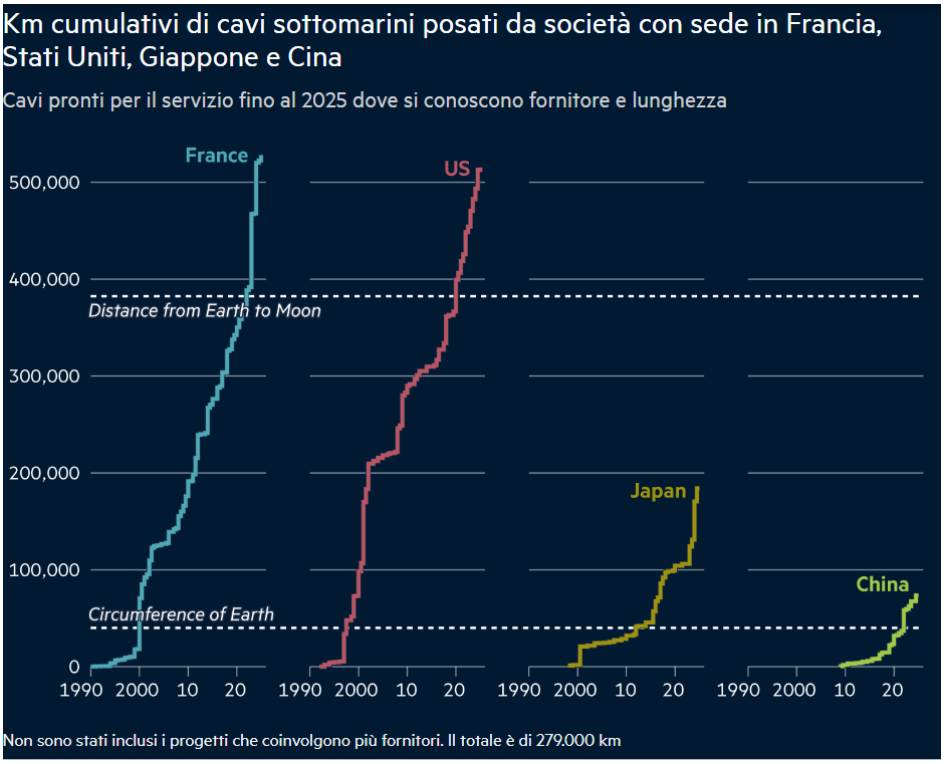


Figura 7: Anna Gross, Alexandra Heal, Chris Campbell et al. "How the US is pushing China out of the internet's plumbing", Financial Times, 13 giugno 2023

[391]M. Turato, **I cavi sottomarini al centro della battaglia tecnologica tra Usa e Cina, Formiche.net, 26 marzo 2023. Accessibile a** https://formiche.net/2023/03/cavi-sottomarini-competizione-usa-cina/#:~:text=I%20cavi%20sottomarini%20sono%20un,dall'intelligenza%20artificiale%20ai%20droni.

4.3.3 L'iniziativa Clean Network

Nel 2020 gli Stati Uniti scoprono le carte e pubblicano l'iniziativa Clean Network con la quale si pongono in guerra aperta con la Cina. L'intento principale è quello di impedire che le entità cinesi diventino il fornitore di base della tecnologia 5G e per questo motivo il governo vieta qualsiasi aiuto statale a quelle aziende che acquisteranno prodotti tecnologici dalle aziende cinesi[392]. L'iniziativa viene accolta favorevolmente dal Congresso che approva anche il Telecommunications Act che dispone 750 milioni di agevolazioni finanziarie per la costruzione dell'infrastruttura 5G. L'iniziativa ha la forma di una dichiarazione politica che viene sottoscritta dai paesi e dalle aziende che vogliono contribuire alla costruzione di un'infrastruttura ICT che escluda le aziende "inaffidabili"[393]. Oltre 60 nazioni di tutto il mondo si sono impegnate pubblicamente a rispettare i principi della "Rete pulita" e tale alleanza è composta da: 27 dei 30 membri della NATO, 26 dei 27 membri dell'UE, 31 dei 37 paesi dell'OCSE, 11 dei 12 paesi dei Tre Mari, nonché Giappone, Israele, Australia, Singapore, Taiwan, Canada, Vietnam, India e Nuova Zelanda. Nonostante i molti paesi firmatari, le reazioni sono state più tiepide di quanto si aspettasse la Casa Bianca. L'Unione Europea ha redatto nel 2020 un documento strategico sul 5G noto come "EU Toolbox on 5G Cybersecurity" in cui non si vietava esplicitamente l'utilizzo di apparecchiature cinesi ma si sottolineava l'importanza di differenziare i rifornitori e che ogni paese dovrebbe valutare quali siano le aziende ad alto rischio. L'iniziativa fa riferimento a 6 settori ICT che dovrebbero essere "puliti" dalle interferenze cinesi: clean carrier, clean store, clean apps, clean cloud, clean cable e clean Telcos. Per quanto concerne i cavi sottomarini, l'obietti è quello di ""garantire che i cavi sottomarini che collegano [gli Stati Uniti] all'Internet globale non vengano sovvertiti per la raccolta di informazioni da parte della Repubblica popolare cinese su scala iper-importante"[394].

Il problema di questo approccio è che rischia di frammentare internet creando un sistema di cavi Occidentale ed uno Orientale a guida cinese con conseguenze drammatiche per la connettività globale e la ridondanza delle comunicazioni. Al centro della contesa vi sono l'Africa ed i paesi in via di sviluppo che rappresentano i mercati in maggior espansione. E' un opinione condivisa da diversi autori, tra cui l'esperta di politica economica estera cinese presso il Center for Naval Analyses, April Herlevi, che il blocco Occidentale e quello Orientale si trovino in una sorta di guerra fredda. Secondo Aprile Herlevi "Non penso che ci siamo ancora arrivati. . . ma temo che questa sia la direzione in cui

[392] Andrzej Dąbrowski, The Clean Network Initiative as an Element of the U.S.-China Competition, The Polish Institute of International Affairs, NO.4 (1700), 8 gennaio 2021. Accessibile a https://www.ceeol.com/search/viewpdf?id=1211210.
[393] Ibidem.
[394] Mike Pompeo, The Clean Network, Dipartimento di Stato, 5 agosto 2020. Accessibile a https://2017-2021.state.gov/the-clean-network/.

stiamo andando"[395]. La complessità dei cavi sottomarini risiede proprio nell'essere un'infrastruttura fortemente interconnessa e sulla quale è difficile, se non impossibile, attuare in modo autonomo la propria strategia. Queste preoccupazioni sono state condivise da diversi membri della comunità digitale. La World Wide Web Foundation (di cui fanno parte Amazon, Facebook, Microsoft, Twitter e altri) ha messo in guardia contro la "frammentazione di Internet" e le "iniziative tecno-protezionistiche", mentre la Internet Society ritiene che "avere un governo che detta le modalità di interconnessione delle reti in base a considerazioni politiche piuttosto che a considerazioni tecniche, è contrario all'idea stessa di Internet"[396]. Alcuni paesi autoritari come la Russia e l'Arabia Saudita hanno testato più volte la possibilità di disconnettere il proprio paese dall'internet globale tramite la costruzione di infrastrutture interne che consentano il completo controllo sui propri cittadini ma sul lungo termine vi sarebbero delle conseguenze disastrose visto il livello di globalizzazione raggiunto da tutti i paesi. Gli stessi Stati Uniti stanno presentando numerose difficoltà dall'estromettere la Cina dalla dorsale internet globale in quanto, ancora oggi, molte delle navi da riparazione o delle aziende che producono tecnologia cruciale per i cavi sottomarini, sono possedute da Pechino. Nessun paese dispone di una flotta dispiegata in tutto il mondo e pronta a salpare per riparare questi cavi, neanche la Cina. Il problema è che la riparazione di un cavo è il momento in cui esso è più vulnerabile ed è più semplice inserire delle backdoor ed estrapolarne i dati. La flotta di sicurezza via cavo (CSF) degli Stati Uniti è composta da due navi via cavo sovvenzionate e di turno. La creazione del CSF sotto l'amministrazione marittima ha rappresentato un significativo passo avanti. Tuttavia, La natura apparentemente autonoma del QCS, il futuro incerto e le risorse limitate rendono discutibile la sua capacità di coordinare una risposta tempestiva e adeguata.

La risposta statunitense all'espansionismo cinese ha avuto un forte impatto sul mercato e la topografia dei cavi sottomarini. Difatti, Pechino vede sempre più aziende escluse dai progetti di carattere globale, anche quando non sono previsti punti di approdo negli Stati Uniti. Questo testimonia come la strategia statunitense non sia puramente difensiva ma miri ad imporre la propria infrastruttura di cavi in tutto il mondo a discapito della Cina. Si può affermare che l'obiettivo a breve termine di frenare la scalata delle aziende cinesi sia stato raggiunto ma allo stesso tempo si nota come Pechino abbia cambiato approccio e rivolga lo sguardo a quei mercati in cui l'influenza americana è meno marcata come quello sudamericano ed africano. Si aggiunga che le aziende cinesi possono offrire prezzi molto più

[395] Ibidem.
[396] "Internet Society Statement on U.S. Clean Network Program," comunicato stampa, Internet Society, 7 agosto 2020, Accessibile a https://www.internetsociety.org/news/statements/2020/internet-society-statement-on-u-sclean-network-program/; "An Open, Interconnected and Interoperable Internet (Joint Letter)," World Wide Web Foundation, September 14, 2021, Accessibile a https://webfoundation.org/2021/09/an-openinterconnected-and-interoperable-internet-joint-letter/.

vantaggiosi rispetto alle controparti occidentali e questo è un elemento decisivo in paesi che hanno un disperato bisogno di infrastrutture.

Inoltre, la crescente ostilità tra la Cina e l'Occidente sta spingendo le aziende a creare nuove rotte lungo le quali inviare il traffico dati. Le controversie sulle acque territoriali, i ritardi nei permessi e il divieto del governo statunitense sui cavi che collegano direttamente la Cina o Hong Kong agli Stati Uniti hanno contribuito a far sì che diversi consorzi di cavi - Apricot, Bifrost ed Echo - forgiassero un nuovo percorso attraverso Singapore, Indonesia, Filippine e il territorio insulare statunitense di Guam, che sta emergendo come un hub per il traffico internazionale di dati.

CAPITOLO 5

Infrastrutture critiche e sicurezza nazionale: il ruolo dei cavi sottomarini per l'Europa e l'Italia

5.1 L'APPROCCIO ITALIANO AL DOMINIO SUBACQUEO

L'Italia è un Paese ontologicamente marittimo per via della sua storia, cultura e posizione geografica. Il Paese si proietta dal Centroeuropa nel bacino Mediterraneo sino al crocevia baricentrico e strategico dello Stretto di Sicilia, pressoché equidistante da Gibilterra, Suez e dagli Stretti turchi, tutti passaggi fondamentali per le principali linee di comunicazione marittima. Questo rapporto intrinseco con il mare è dimostrato anche dai numeri. Le coste del Paese sono lunghe oltre 8.500 chilometri, pari a circa l'87% dei confini esterni dell'Italia, e rappresentano una fonte di opportunità economiche e un ponte verso gli oceani del mondo ed il commercio globale[397]. Infatti, il 64% delle importazioni e il 50% delle esportazioni dell'Italia sono trasportate via mare, mentre 480 milioni di tonnellate di merci transitano annualmente nei porti del Paese[398]. Nel 2018, la "blue economy" italiana impiegava oltre mezzo milione di persone, per un fatturato complessivo di 82,2 miliardi di euro, un valore aggiunto di 23,8 miliardi di euro a fronte di investimenti per soli 2,4 miliardi[399]. L'Italia, possedendo

[397] Fondazione Leonardo e Marina Militare Italiana, Civiltà del mare. Geopolitica, strategia, interessi nel mondo subacqueo. Il ruolo dell'Italia, 2022, pp. 24
[398] Ibidem.
[399] Addamo, A., Calvo Santos, A., Carvalho, N., et al. The EU blue economy report Commissione Europea, Direzione Generale degli Affari marittimi e della pesca, Centro Comune di Ricerca, Ufficio delle pubblicazioni dell'Unione Europea, 2021.

un'economia proiettata all'attività di trasformazione dei materiali[400], è particolarmente dipendente dall'import ed export che transitano, rispettivamente, per il 64% ed il 50% via mare[401]. Per quanto concerne il commercio marittimo, il Mediterraneo è un crocevia nevralgico: rappresenta l'1% della superficie marittima mondiale ma al suo interno vi passa circa il 20% del traffico marittimo mondiale, il 25% dei servizi di linea su container, il 30% dei flussi di petrolio mondiali, il 65% del flusso energetico per i paesi dell'Unione Europea[402]. Il Mediterraneo allargato presenta una faglia tra un Nord sviluppato e un blocco frastagliato con un Sud tradizionalmente fragile sul piano politico, sociale ed economico, sovrappopolato e conflittuale, un Nord-Est caratterizzato da una rinnovata postura assertiva sul piano politico-militare e un Oriente (vicino e medio) in cui si osserva una pronunciata competizione tra diverse realtà politiche, statuali o non statuali[403].

La proiezione marittima dell'Italia è stata confermata anche dall'esecutivo di Giorgia Meloni sotto il quale ha preso vita il nuovo Ministro per la Protezione Civile e le Politiche del Mare che si occupa del coordinamento inter-agenzia dei vari ministeri che si occupano di tematiche relative al mare. Sotto la supervisione di questo Ministero è stato pianificato il Piano per il Mare del triennio 2023-2025 che è il principale documento strategico in questo ambito. Tuttavia, si registra la bassa se non inesistente attenzione che viene data ai cavi sottomarini in fibra ottica all'interno di questo rapporto. Basti pensare che su un totale di 236 pagine, il termine "cavo sottomarino" viene citato soltanto 13 volte ed in termini particolarmente generali. Diversa attenzione viene data dalla Marina Militare che in due documenti di carattere strategico ha sottolineato più volte il ruolo strategico dei cavi sottomarini e le linee guida per la loro protezione[404].

5.1.1 Polo di Innovazione Nazionale per il Subacqueo

Il dominio subacqueo è strategico per gli interessi italiani ma per averne consapevolezza e controllo sono necessari degli importanti sviluppi tecnologici che non possono provenire esclusivamente dalla ricerca condotta da enti statali. I soggetti privati giocano un ruolo cruciale nello sviluppo dei droni subacquei il cui utilizzo può essere sia di natura civile che militare. Un esempio è quello dell'AUV FlatFish prodotto da Saipem che è in grado di eseguire autonomamente ispezioni di asset

[400] L'Italia è il primo polo manifatturiero di Cavi e Conduttori Elettrici e siamo la terza industria manifatturiera. Vedi La Stampa, "l'Italia è il primo polo manifatturiero in Europa per la produzione di cavi e conduttori elettrici", Ultima modifica 17 Novembre 2023.
[401] Fondazione Leonardo, Marina Militare Italiana, Rapporto Civiltà del Mare, 2022, pp. 25.
[402] Ivi.
[403] Ibidem, pp.23.
[404] Marina Militare, Linee di Indirizzo Strategico 2019-2034, Rivista Marittima, 2019. Vedi anche Rapporto Marina Militare 2022, 2023. Accessibile a https://www.marina.difesa.it/Documents/rapporto_mm_2022_.pdf.

sottomarini[405]. La sua peculiarità è quella di operare grazie ad una sorta di garage subacqueo installato sul fondale marino dove il drone ricarica le sue batterie senza dover tornare su una nave madre.

Grazie alla presenza di numerose strutture civili, militari e industriali, la città di La Spezia sta diventando un vero e proprio hub per lo sviluppo di soluzioni tecnologiche e operative legate al dominio subacqueo. È sede di numerose aziende che si occupano di tecnologia subacquea, oltre che del CMRE della NATO e del Centro di supporto e sperimentazione navale (CSSN) della Marina Militare Italiana e del Comando Raggruppamento Subacquei e Incursori Teseo Tesei (COMSUBIN). Inoltre, La Spezia ospiterà presto il nuovo Polo nazionale della dimensione subacquea (PNS), che avrà sede all'interno del centro prove della Marina Militare già esistente in città. Il progetto nasce dall'esigenza di mettere a sistema le varie realtà che operano nel settore dell'Underwater, dal campo della ricerca scientifica a quello della sicurezza. Il settore subacqueo, infatti, pur contando su un pregiato e variegato portfolio di capacità e progettualità risente di una forte frammentazione del settore. Il Polo è stato istituito tramite un apposito Decreto del Ministero della Difesa, di concerto con il Ministero dell'Università e della Ricerca ed il Ministero delle Imprese e del Made in Italy e gli è stata anche assegnata una prima dotazione finanziaria per il funzionamento e le attività di innovazione tecnologica. Pertanto, la Marina Militare agirà da apripista e avrà un ruolo cruciale nella governance dell'Istituto. Il Polo Nazionale della dimensione Subacquea (PNS) agirà da incubatore per spin-off e start-up che restituiranno alta competitività, anche internazionale, alle aziende italiane.

5.1.2 Risorse e strategie della Marina Militare Italiana per l'Underwater ed i cavi sottomarini

Dal punto di vista della difesa, la dimensione subacquea, che si estende da appena sotto la superficie fino al fondo marino, è ora considerata dalla MMI come il quinto dominio operativo fisico, accanto a quello aereo, terrestre, marittimo e spaziale. Questa visione è radicata nelle peculiarità dell'ambiente subacqueo, dove le soluzioni di comunicazione che funzionano sopra la superficie e nello spazio sono fortemente limitate, alterate o negate, dai vincoli fisici inerenti all'operare all'interno di uno specchio d'acqua, riguardanti la visibilità e la limitata capacità di trasferimento dei dati. La Marina italiana considera la guerra subacquea come comprendente ASW (Anti-submarine Warfare), guerra di mine e guerra sui fondali marini, ed è intenzionata a gettare le basi per una revisione della dottrina sia a livello nazionale che a livello NATO. In particolare, l'ambiente subacqueo rende estremamente impegnativa la capacità di comunicare con i sottomarini e di controllare i mezzi non equipaggiati che operano in profondità. Pertanto, si ritiene che operare sott'acqua richieda un nuovo approccio

[405] Saipem, Flatfish, aprile 2023, https://www.saipem.com/sites/default/files/2023-04/Flatfish.pdf; Saipem, Saipem Subsea Drone for Inspection of Shell and Petrobras Fields in Brazil, 24 maggio 2022, https://www.saipem.com/en/media/press-releases/2022-05-24/saipem-subsea-droneinspection- shell-and-petrobras-fields-brazil.

dottrinale, nonché competenze e soluzioni tecnologiche diverse da quelle utilizzate nelle operazioni di superficie, soprattutto se si considera che l'uso degli UUV ha spinto i confini in termini di modalità di funzionamento delle marine militari in profondità e degli attori privati. Secondo la MMI, il primo passo necessario è il perseguimento di un'adeguata consapevolezza situazionale sottomarina, un concetto simile a quelli applicati agli altri domini operativi ma più difficile da implementare a causa dei suddetti vincoli fisici e tecnologici. Questa potrebbe essere sviluppata creando una rete subacquea composta da nodi interoperabili che comunicano tra loro.

Una delle maggiori difficoltà nel proteggere i cavi sottomarini è data dall'ambiente subacqueo nel quale essi si trovano. Un ambiente le cui proprietà fisiche mettono a dura prova le tecnologie esistenti al pari dello spazio. L'uomo è l'anello debole di questo ecosistema e necessita di veicoli che lo proteggano dalle fortissime pressioni indotte dall'acqua. Tuttavia, anche i veicoli devono affrontare delle grandi sfide tecnologiche dal punto di vista operativo. Innanzitutto, c'è un problema di rifornimento: per funzionare i sottomarini e gli UUV devono fare i conti con la necessità di aria per la ricarica dei motori a Diesel[406] ed il poco spazio a disposizione. La ricerca tecnologica si sta concentrando su come diminuire la grandezza delle batterie elettriche ed aumentarne il range di autonomia[407]. Tuttavia, non è possibile pensare che i droni possano funzionar esclusivamente in presenza di un natante che li raccolga al suo interno. Per tali ragioni si sta ragionando sulla creazione di piattaforme stabili posizionate sui fondali marini da cui questi sistemi possano partire e tornare per rifornirsi[408]. Inoltre, vi è un problema di comunicazione sott'acqua in quanto la tecnologia wireless non può funzionare. Difatti, le onde elettromagnetiche non riescono a penetrare l'acqua e sono utilizzabili solo le onde acustiche o le onde radio a bassissima frequenza. Tra le vittime dell'ambiente marittimo vi è anche il Global Positioning System (GPS) motivo per il quale i sottomarini devono calcolare la loro posizione tramite sistemi di navigazione inerziale[409]. Per risolvere questo problema si stanno sviluppando nuove tecnologie come il "Positioning System for Deep Ocean Navigation" (POSYDON)[410] che si basa su una serie di sensori acustici. Gli Stati Uniti son ben consapevoli

[406] D. Archus, How Do Submarines Navigate Underwater?, Naval Post, 13 maggio 2021.
[407] M. Battaglia, Difesa underwater. Buttitta (Engineering) presenta le nuove tecnologie sottomarine, Formiche.net, 15 Giugno 2023. Accessibile a https://formiche.net/2023/06/difesa-underwater-buttitta-engineering-presenta-le-nuove-tecnologie-sottomarine/.
[408] "le piattaforme, compresi i sottomarini, dovrebbero evolvere in "hub strategici" per generare la massa critica e gli effetti necessari laddove richiesto, anche attraverso il lancio e il recupero di UUV e AUV". Vedi Marina Militare Italiana, Future Combat Naval System 2035 nelle operazioni Multi Dominio, pp. 2.
[409] Il sistema di navigazione inerziale è un sistema di guida ausiliario per la misurazione dell'accelerazione e della velocità angolare di un oggetto in movimento con l'utilizzo di un accelerometro e di un giroscopio e con l'applicazione di tecnologia computerizzata.
[410] Si tratta di un progetto annunciato nel 2015 dall'ente governativo statunitense DARPA. Vedi N. Trausti Fridbertsson, Protecting Critical Maritime Infrastructure – The Role of Technology, Nato Parliamentary Assembly – Science and Technolgy Committee, 6 Aprile 2023, pp. 8. Accessibile a https://www.nato-pa.int/download-

dell'importanza di questo settore e degli sforzi tecnologici di cui necessita motivo per il quale è stata creata appositamente la Task Force 59 con lo scopo di creare un "Oceano Digitale" composto da una "rete integrata di sensori e sistemi senza pilota" in grado di segnalare attività insolite[411].

La Marina Militare Italiana ha intenzione di muoversi in questa direzione e ciò si vede chiaramente nel documento "Future Combat Naval System 2035 in Multi Domain Operations" all'interno del quale vi è uno specifico riferimento al dominio subacqueo[412]. L'obiettivo fondamentale è quello di sviluppare veicoli dotati di grande autonomia[413] ma che allo stesso tempo siano in grado di funzionare in stretta collaborazione con gli altri sistemi unmanned. Un ruolo chiave sarà giocato dall'Intelligenza Artificiale (IA) che potrebbe garantire un'analisi dei dati raccolti sempre più veloce e precisa[414].

Al momento della stesura del documento, la MMI sta già operando con diversi AUV, tra cui l'HUGIN 1000 (prodotto da Kongsberg e in grado di raggiungere i 3.000 metri di profondità) e i REMUS 100 e 300, e sta valutando le capacità future tenendo conto dell'esperienza della dimostrazione in mare nel contesto del progetto OCEAN2020.

Tra le unità militari utilizzate per la difesa delle infrastrutture critiche vi sono anche i sommergibili su cui l'Italia ha intenzione di investire notevoli risorse. Il programma di punta della Marina Militare Italiana è il nuovo sottomarino U212 Near Future Submarine (NFS) la cui costruzione avverrà in loco tramite Fincantieri. Il valore complessivo del progetto è di 2,3 miliardi ed i tre sottomarini dovrebbero essere consegnati tra il 2027 ed il 2029[415]. Il Programma nasce dall'esigenza di garantire un'adeguata capacità di sorveglianza e controllo dello spazio subacqueo, con compiti che spazieranno da missioni puramente militari ad operazioni relative alla libertà di navigazione, all'antipirateria, alla sicurezza delle rotte di approvvigionamento energetico, alla lotta al terrorismo, alla difesa delle frontiere esterne

file?filename=/sites/default/files/2023-04/032%20STC%2023%20E%20-%20CRITICAL%20MARITIME%20INFRASTRUCTURE%20-%20FRIDBERTSSON%20REPORT.pdf

[411] Ivi.

[412] Marina Militare Italiana, Il Future Combat Naval System 2035 nelle operazioni multi-dominio, 2021, Accessibile a https://www.marina.difesa.it/media-cultura/Notiziario-online/Documents/Il%20Future%20Combat%20Naval%20System%202035.pdf .

[413] Con il termine "veicoli" si fa riferimento ai veicoli di superficie senza equipaggio (USV), ai veicoli di superficie autonomi (ASV) e gli Unmanned Underwater Vehicles (UUV). Per approfondire vedi Y. Allard, E. Shahbazian, Unmanned Underwater Vehicle (UUV) Information Study, OODA Technologies Inc, Defence Research & Development Canada (Atlantic Research Centre), 28 Novembre 2014.

[414] N. Trausti Fridbertsson, Protecting Critical Maritime Infrastructure – The Role of Technology, Nato Parliamentary Assembly – Science and Technolgy Committee, 6 Aprile 2023. Accessibile a https://www.nato-pa.int/download-file?filename=/sites/default/files/2023-04/032%20STC%2023%20E%20-%20CRITICAL%20MARITIME%20INFRASTRUCTURE%20-%20FRIDBERTSSON%20REPORT.pdf

[415] C. Rossi, Fincantieri, Tutti i Lavori sul Primo Sottomarino Nfs per la Marina, Startmag, 11 Gennaio 2022.

ed alla salvaguardia delle infrastrutture marittime, comprese le infrastrutture essenziali offshore e subacquee[416]

5.2 LE CRITICITA' ED I PUNTI DI FORZA DEI CAVI SOTTOMARINI ITALIANI

La posizione mediana nel Mediterraneo rende l'Italia un perfetto hub commerciale ed energetico della regione. Non è quindi un caso che per i nostri territori già passino importantissimi gasdotti che portano direttamente ai produttori di gas come nel caso del Gasdotto Trans-Mediterraneo (che collega la Sicilia all'Algeria passando per la Tunisia), il Gasdotto Greenstream (che collega la Libia all'Italia) e infine il Gasdotto Trans-Adriatico (TAP), che collega la costa pugliese all'Azerbaigian passando per l'Albania, la Grecia e la Turchia[417].

Anche per quanto concerne i cavi sottomarini in fibra ottica l'Italia rappresenta un centro nevralgico del Mediterraneo. Un punto di snodo per la maggior parte delle comunicazioni tra Europa, Africa ed Asia. Nel Nord Est si trova il cavo Italia-Croazia che risale al 1994 mentre sempre nell'Adriatico la città di Bari rappresenta un punto di approdo di diversi cavi, tra cui quello Italia-Albania sempre costruito nel 1994. E' doveroso menzionare due cavi di rilevanza regionale e globale. Il primo è il cavo Jonah, del 2012, lungo 2.297 km, sviluppati tra Tel Aviv (Israele) e l'Italia. Il secondo, è un cavo di rilevanza globale, la cui lunghezza complessiva è di oltre 25.000 km. L'infrastruttura in questione è l'Asia Africa Europe-1 (AAE-1), che si dipana tra Cape d'Aguilar (Cina) e Marsiglia (Francia). L'infrastruttura, oltre ai due punti di origine, tocca terra in altre 18 località, servendo altrettanti paesi.

[416] U212 NFS, OCCAR, Accessibile a https://www.occar.int/our-work/programmes/u212-nfs.

[417] Global Energy Monitor, Global Gas Infrastructure Tracker - Tracker Map, https://globalenergymonitor.org/projects/global-gas-infrastructure-tracker/tracker.

Figura 32: Fonte: Global Energy Monitor, Global Gas Infrastructure Tracker – Tracker Map, cit.

Il cavo parte come detto dalla Cina passando per il Sud-Est asiatico, l'India, i Paesi del Golfo e giunge nel Mediterraneo attraverso il Mar Rosso, arrivando in Italia appunto a Bari. Alcune delle propaggini dell'AAE-1 sarebbero state oggetto del sabotaggio registrato a Marsiglia nel mese di ottobre 2022[418]. Data l'estensione geografica dell'infrastruttura, il suo danneggiamento ha causato a cascata, disagi in tutti i paesi attraversati dall'AAE-1.

Il Sud Italia è la zona dove troviamo i più importanti punto di approdo. Sulla costa tirrenica è presente un cavo via terra e via mare i cui capi sono entrambi sul suolo italiano: è il Janna, che si dipana da Civitavecchia ad Olbia, per poi proseguire via terra in Sardegna fino a Cagliari e nuovamente via mare fino a Mazara del Vallo (Sicilia)[419]. Altri due hub logistici fondamentali per il network delle telecomunicazioni italiane sono quelli di Genova e Savona. Il centro della connettività del Paese con i network regionali e globali è individuabile lungo le coste della Sicilia. Palermo è connessa a due infrastrutture globali come il FLAG Europe-Asia (FEA) che origine nella città di Miura (Giappone) e tocca 13 paesi prima di terminare la propria corsa a Porthcurno (Regno Unito) per una lunghezza totale di 28.000 km. Altro snodo cruciale è rappresentato dalla città di Mazara del Vallo in cui atterrano sei cavi di diversa importanza. Alcuni cavi sono di carattere regionale e collegano l'Italia con il Nord Africa (Tunisia e Libia)[420] mentre l'infrastruttura principale a cui è connessa la città è il

[418] Eurispes, 35° Rapporto Italia – Percorsi di Ricerca nella Società Italiana, 2022, pp. 795.
[419] Ivi.
[420] Si fa riferimento ai cavi Didon (170 km, Italia – Tunisia), l'Hannibal System (179 km, Italia – Tunisia), il GO-Mediterrean Cable System (290 km, Italia- Malta).

cavo SeaMeWe-3 che si distende per 39.000 km da Ostenda (Belgio) a Perth (Australia). Il cavo interessa il continente asiatico, africano ed europeo ed è uno dei più lunghi al mondo. Infine, la città di Catania ospita due cavi particolarmente rilevanti, il MedNautilus Submarine System ed il SeaMeWe-5. Il primo è rilevante per via della tratta che collega Italia, Israele, Cipro, Grecia e Turchia offrendo una valida alternativa alla più comune rotta che passa per l'Egitto. Difatti, Israele può rappresentare uno snodo cruciale per quei cavi che puntano ad arrivare nel Mar Rosso senza passare tramite il Canale di Suez per via dei pericoli che presenta questo collo di bottiglia dal punto di vista geopolitico. Il secondo, è tra i cavi più lunghi al mondo (20.000 km) ed interconnette sedici paesi a livello globale, dalla Francia all'Italia, passando, anche questo, per i Paesi del Golfo, lo Sri Lanka, il Bangladesh e concludendo il proprio percorso a Tuas (Singapore).

Come si può facilmente notare, i percorsi sono molto simili tra loro. I cavi globali passano dall'Italia per allungarsi verso il canale di Suez e dirigersi verso il Mar Rosso e l'Asia mentre i cavi regionali connettono l'Italia con i paesi che affacciano sul Mediterraneo come la Tunisia, la Libia e Malta.

Città di collegamento	Denominazione cavo	Lunghezza complessiva	Anno di realizzazione
Mestre	*Italia-Croazia*	230 km	1994
Bari	*Italia-Albania*	240 km	1994
Bari	*OTEGLOBE Kokkini-Bari*	350 km	2004
Bari	*Jonah*	2.297 km	2012
Bari	*Asia Africa Europe-1*	25.000 km	2017
Otranto	*Italy-Greece-1*	169 km	1995
Civitavecchia	*Janna*	634 km	2005
Genova	*Medloop*	-	2022
Savona	*Italy-Monaco*	162 km	1995
Palermo	*FLAG Europe-Asia*	28.000 km	1997
Palermo	*SeaMeWe-4*	20.000 km	2005
Trapani	*Trapani-Kelibia*	209 km	1995
Mazara del Vallo	*Didon*	170 km	2014
Mazara del Vallo	*Hannibal System*	178 km	2009
Mazara del Vallo	*GO-1 Mediterranean Cable*	290 km	2008
Mazara del Vallo	*Italy-Libya*	570 km	1998
Mazara del Vallo	*MENA System/Gulf Bridge*	8.000 km	2014
Mazara del Vallo	*SeaMeWe-3*	39.000 km	1999
Marina di Ragusa	*Malta Italy Interconnector*	95 km	2015
Pozzallo	*Melita 1*	97 km	2009
Catania	*EMSCS*	260 km	2004
Catania	*Italy-Malta*	238 km	1995
Catania	*MedNautilus Submarine*	7.000 km	2001
Catania	*IMEWE*	12.091 km	2010
Catania	*SeaMeWe-5*	20.000 km	2016

Figura 33: Eurispes, Rapporto Italia 2023, pp. 800.

5.2.1 Progetti Futuri

Oltre ai cavi citati, vi sono dei progetti particolarmente rilevanti sia in termini tecnologici che per la loro lunghezza che saranno completati entro pochi anni. Ci si riferisce al cavo Medusa che collegherà Port Said, in Egitto, a Lisbona, in Portogallo per una lunghezza totale di 7.100 km entro il 2025. Questo sistema di cavi sarà dotato di una tecnologia di monitoraggio intelligente nota come

Distributed Acoustic Sensing (DAS)[421]. Si tratta di un sistema di sensori acustici che fornirà un allarme precoce in caso di attività potenzialmente minacciose per l'infrastruttura[422]. Nel frattempo, un progetto separato, denominato BlueMed, collegherà un'importante piattaforma di atterraggio dati a Genova con il Mar Rosso, passando per un hub di dati a Palermo e attingendo a una rete più ampia che tocca Francia, Grecia e Israele, oltre ad altri cavi nella regione[423]. Parallelamente a questi due progetti si sta lavorando per far approdare a Genova il cavo più lungo al mondo, il 2Africa che avrà una lunghezza di 45.000 km e circumnavigando il continente africano connetterà 3,2 miliardi di persone. Parallelamente a questi progetti, il nostro paese sta sviluppando un cavo strettamente locale noto come "Collegamento Isole Minori" che vede la partecipazione di Infratel S.p.A ed Elettra Tlc[424]. L'obiettivo è quello di collegare 21 isole tra il Lazio, la Puglia, la Sicilia, la Toscana e la Sardegna che ad oggi sono collegate unicamente da ponti radio.

L'Italia si conferma un paese di approdo di numerosi cavi sia regionali che globali, specialmente per quanto riguarda le tratte che portano al Nord Africa e l'Asia. Di contro, non vi sono cavi che connettano direttamente il paese con il continente americano che invece hanno origine in Francia, Spagna e Regno Unito. Un altro problema è rappresentato dalla scarsa differenziazione dei punti di approdo che sono localizzati in sole undici città e per il 60% in sole tre località, Mazara del Vallo, Bari e Catania. Inoltre, l'Italia risulta essere in ritardo rispetto ad altri paesi europei per via della mancanza di cavi che nascono direttamente sul suo territorio.

Alla luce di quanto detto, il sistema di cavi sottomarini italiani risulta, come quelli di altri paesi europei, interdipendente dalle maggiori reti di distribuzione a livello globale, ovvero quelle reti che hanno i propri hub principali a Marsiglia, nel Regno Unito, in Giappone ed in Cina. Ciò presenta diversi problemi per la sicurezza delle nostre connessioni e ci espone maggiormente ad eventi come quelli recentemente avvenuti presso le isole Svalbard o a Marsiglia dove il danneggiamento di pochi cavi ha causato un rallentamento delle connessioni in diversi paesi. L'Italia dovrebbe prendere molto seriamente queste minacce per via della presenza sempre più assidua nei mari di nostra competenza della Marina Militare Russa, le cui competenze nell'ambito del sabotaggio e spionaggio di cavi sottomarini è ormai nota. A differenza dei cavi energetici in cui è individuabile un paese donatore ed

[421] SAGE, Distributed Acoustic Sensing (DAS) Research Coordination Network (RCN). Per maggiori informazioni vedi https://www.iris.edu/hq/initiatives/das_rcn.
[422] Direzione generale della Commissione europea per i negoziati di vicinato e di allargamento, The Medusa Submarine Cable System - Factsheet, 24 novembre 2022, Accessibile a https://neighbourhood-enlargement.ec.europa.eu/node/4194_en.
[423] Ministero degli Affari Esteri italiano, Con BlueMed, Sparkle crea a Genova un nuovo hub digitale per il traffico internet globale, 1 marzo 2023, Accessibile a https://www.esteri.it/en/?p=97536.
[424] Infratel, Banda ultralarga per le isole minori: via al cantiere delle tratte sottomarine, 20 novembre 2023. Accessibile a https://www.infratelitalia.it/archivio-news/notizie/bul-per-le-isole-minori

uno ricevente, i cavi sottomarini fungono da connettori tra diversi paesi e ciò comporta che le soluzioni per la loro sicurezza debbano essere trovate in una maggiore collaborazione internazionale, in primis a livello europeo.

5.3 SPIONAGGIO SOTTOMARINO: LE OPERAZIONI TEMPORA E PRISMA

I dati sono diventati elemento essenziale in moltissimi settori. Possedere i dati significa possedere le informazioni e avere una maggiore consapevolezza del campo di battaglia (qualunque esso sia, economico, politico o militare). Ad oggi le informazioni non passano più di mano in mano tramite valigette o documenti ma tramite strumenti elettronici che per funzionare necessitano principalmente di un'infrastruttura critica, i cavi sottomarini. L'intelligence si è sempre più adattata a questo cambio di paradigma passando da una raccolta e analisi delle informazioni basata sull'uomo ad un sistema in cui le tecnologie ne fanno da padrona tramite l'utilizzo dei satelliti e dell'Intelligenza Artificiale. Sebbene gli eventi recenti abbiano dimostrato come la tecnologia non sia in grado di prevenire le minacce in modo infallibile, rimane comunque il fatto che la maggior parte delle comunicazioni mondiali passa attraverso i cavi e ciò li rende lo spazio privilegiato per lo spionaggio. Il caso che più di tutti ha reso evidente come i governi ed i servizi di sicurezza si concentrino sempre più sulla ricerca di una grande mole di dati è stato il Datagate svelato da Edward Snowden[425]. L'ex dipendente della National Security Agency (Nsa), svela l'esistenza di due programmi speciali per il monitoraggio del cyber spazio, Mastering the Internet e Global Telecoms Exploitation. Inoltre, ne cita un terzo che assume rilevanza perché ideato per l'intercettazione dei dati trasmessi attraverso i cavi in fibra ottica: il nome in codice è Tempora ed è stato testato nel 2008 e diventato operativo nel 2011. Il programma sarebbe stato ideato e finanziato insieme alla National Security Agency (NSA) statunitense[426] e, secondi alcuni analisti, vi sarebbe stato un tacito accordo con le compagnie di telecomunicazioni mondiali per l'accesso ai dati da loro veicolati come avvenuto nel caso del progetto PRISMA. Quest'ultimo progetto è stato reso operativo dal 2007 e si basava su una partnership pubblico-privato resa possibile da una legge del 1978, la section 702 del Foreign Intelligence Surveillance Act (FISA)[427]. Secondo questa legge, l'amministrazione può chiedere ad una corte speciale di sorvegliare

[425] Ewen MacAskill, Julian Borger, Nick Hopkins, GCHQ taps fibre-optic cables for secret access to world's communications, The Guardian, 21 giugno 2013. Accessibile a https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa .
[426] Si tratta dell'agenzia statunitense che si occupa di SIGINT (sigla che sta per *SIGnal INTelligence,* ossia spionaggio di sistemi elettromagnetici).
[427] N. De Scalzi, Lo Spionaggio Informatico del Progetto Prisma e Tempora, Treccani, 10 luglio 2013. Accessibile a https://www.treccani.it/magazine/atlante/geopolitica/Lo_spionaggio_informatico_del_programma_PRISM.html.

le comunicazioni di un cittadino non statunitense che si trovi all'estero[428]. Una volta ottenuta l'approvazione da parte della Corte, la NSA può richiedere le informazioni direttamente alle aziende che, a loro volta, possono far ricorso alla Corte speciale. Qualora il ricorso non venne accettato, le compagnie avrebbero l'obbligo di collaborare con l'NSA. Alcune delle aziende coinvolte, come Google e Facebook, hanno acconsentito anche alla richiesta di creare delle vere e proprie stanze fisiche, all'interno delle aziende, dove vengono collocati server per l'archiviazione di metadati (informazioni che descrivono altri insiemi di dati[429])[430]. David Drummond, capo dell'ufficio legale di Google, ha detto che lo scambio di informazioni con l'NSA avveniva grazie ad un semplice programma di condivisione crittografato chiamato "File Transfer Protocol" (FTP)[431]. Sempre secondo il New York Times, solo nel 2012 sarebbero pervenute 1856 richieste di informazioni alle aziende. Il progetto PRISMA già prevedeva uno scambio di informazioni con il Government Communications Head Quarter (GCHQ), la controparte inglese della NSA. Il Progetto Tempora è stato un'estensione del progetto Mastering the Internet del 2007 grazie al quale, sempre secondo il Guardian, il GCHQ avrebbe raccolto metadati su oltre 600.000 eventi telefonici transitati attraverso 200 cavi a fibra ottica al giorno per 18 mesi[432]. Ciascun cavo trasporta circa 10 gigabits al secondo, oltre 21 petabites al giorno. La raccolta di metadati ha interessato anche messaggi emails, accessi a profili Facebook e siti internet di oltre 2 miliardi di utenti. L'attività di raccolta dei dati sarebbe stata gestita presso la base di Crooklets Beach a Bude, a Widemouth Bay, in Cornovaglia[433], dove afferiscono numerosi cavi sottomarini[434]. Anche il progetto inglese si basava su leggi esistenti, nello specifico il Regulation of Investigatory Powers Act (RIPA) che consente lo spionaggio su targets specifici sulla base di criteri relativi alla sicurezza nazione, la protezione da minacce terroristiche e la difesa del benessere economico dello stato. A differenza della legislazione statunitense, i targets sorvegliabili devono trovarsi sul territorio inglese. Tuttavia, i cavi in fibra ottica consentono di aggirare questo limite dal momento che i dati di un soggetto possono passare per un server inglese pur partendo dall'estero. D'altronde, il RIPA era stato ideato 13 anni prima quando le tecnologie di spionaggio erano molto

[428] Secondo il "Protect America Act" (PAA) firmato da George Bush nel 2007, la NSA può sorvegliare le informazioni tra terminal all'estero anche se passano da server che si trovano fisicamente sul territorio statunitense, senza violare il IV emendamento della Costituzione americana che regola il diritto alla privacy.
[429] Il metadato, ('dato oltre un altro dato'), è un'informazione che descrive un insieme di dati. I campi presenti in una collezione di metadati sono rappresentati da informazioni che indicano precisamente le risorse informative a cui si applicano, con lo scopo di migliorarne la visibilità
[430] N. De Scalzi, Progetto Prisma e Tempora, 2013, Treccani.
[431] C. Cain Miller, 3 giganti della tecnologia vogliono rivelare le richieste di dati, The New York Times, 3 giugno 2013. Accessibile a https://www.nytimes.com/2013/06/12/technology/google-asks-to-reveal-details-about-classified-requests.html?_r=0 .
[432] N. De Scalzi, Progetto Tempora e Prisma, Treccani, 2013.
[433] A. Teti, Spionaggio Sottomarino – Attività di Intelligence e siti segreti, Gnosis, Marzo 2014.
[434] Si tratta di: Apollo /Usa; Tat-3 /Usa; Cantat-1 /Canada; Tat-8 /Usa e Francia; Tat-14 /Usa e Europa; Ac-2 /Usa; Gie /Europa e India; Glo-1 /Africa occidentale.

diverse. Ad ogni modo, la collaborazione con l'NSA serviva proprio ad aggirare eventuali limiti legislativi interni ai due paesi: la sorveglianza che non era consentita ad uno paese era possibile dall'altro e a quel punto bastava uno scambio di informazioni per poter accedere alla quasi totalità di dati disponibili.

Il progetto Tempora utilizzava un apposito software ideato dalla NSA[435] che, tramite l'analisi dei metadati, sarebbe in grado di creare una conoscenza strutturata su un determinato evento, scenario o individuo, in tempo reale. Per questo esso sarebbe definito dall'agenzia statunitense come Digital Network Intelligence (Dni). Il suo utilizzo e la sua architettura sono stati rivelati dal "The Sydney Morning Herald"[436] e dal giornale "O Globo" a testimonianza di come il progetto coinvolgesse anche gli altri partner dell'alleanza Five Eyes[437]. Per sfruttare al massimo le potenzialità di Xks, la Cia e la Nsa hanno creato le seguenti strutture 'ibride' ove confluiscono i migliori tecnici specializzati nell'analisi dei metadati: Special Collection Service (Scs) che ha il suo quartiere generale a Beltsville, nel Maryland (il cui palazzo s'affianca a quello del State Department's Beltsville Communications Annex, la struttura che afferisce al Diplomatic Telecommunications Service e si occupa delle comunicazioni criptate delle stazioni Cia nel mondo)[438]; Foreign Satellite Interception (Fornsat), dedicata all'intercettazione delle comunicazioni dei satelliti stranieri, che si baserebbe su almeno 52 stazioni di ascolto, alcune delle quali note[439] ; Special Source Operations (Sso), specializzata nell'intercettazione dei dati veicolati sui cavi sottomarini in fibra ottica. Non è conosciuto quali e quante siano le stazioni dello Sso operanti a livello planetario ma, da fonti aperte, sembrerebbe che le maggiori attività di analisi siano incentrate sui punti di approdo dei cavi sottomarini che collegano Indonesia, Corea del Sud, Guam, Isole Caroline, Hawaii, Stati Uniti, Gran Bretagna, Francia, Gibuti, Oman, Afghanistan.

5.3.1 Le fragilità dei punti di approdo nel Mediterraneo

Sempre nel 2013 Snowden afferma che il punto di approdo di Mazara del Vallo sarebbe stato ripetutamente violato dal GCHQ e dall'NSA. Mazara del Vallo è un punto nevralgico sia per l'Italia che per il Mediterraneo dal momento che vi passano alcuni tra i cavi più lunghi al mondo come il

[435] Il software in questione si chiama Xks e si baserebbe su una multipiattaforma di server di tecnologia avanzata.
[436] P. Dorling, X-Keyscore spy program tracks 'nearly all' web use, The Sydney Morning Herald, 2 agosto 2013. Accessibile a https://www.smh.com.au/technology/xkeyscore-spy-program-tracks-nearly-all-web-use-20130802-hv17w.html
[437] Organizzazione cui aderiscono Stati Uniti, Australia, Canada, Regno Unito e Nuova Zelanda.
[438] A. Teti, Spionaggio Sottomarino, Gnosis, 2013.
[439] Tra le stazioni note vi sono quelle di Indra (Khon Kaen, Tailandia), Ladylove (Filippine), Timberline (Sugar Grove, Usa), Carboy (a Bude), Moonpenny (Menwith Hill, Gran Bretagna), Stellar (Geraldton, Australia), Ironsand (Waihopai, Nuova Zelanda), Jackknife (Yakima, Giappone), Sounder (Ayios Nikolaos, Cipro), Snick (Seeb, Oman). Un'altra stazione si troverebbe nei pressi di Skibsbylejren (Danimarca). Vedi A. Teti, Spionaggio Sottomarino, Gnosis, 2013.

SEA-ME-WE 3, SEA-ME-WE-4 e il Flag Europe-Asia (Fea) da cui sarebbero state intercettate 600 milioni di telefonate al giorno. Tra i punti di approdo più noto per lo spionaggio dei cavi vi è quello di Ayios Nikolaos a Cipro dove ha sede un'importantissima base di ascolto gestita da Stati Uniti e Regno Unito. Il suo sviluppo trae origine da un progetto del 2012, denominato Operazione Mullenize, in cui si evidenzia la necessità di condurre attività d'intercettazione dati in internet 440. Nell'articolo che ha portato alla ribalta questa operazione sono citate tre basi operative di riferimento: Benhall, Bude e Sounder. Quest'ultimo nome corrisponde al codice di copertura della base di Ayios Nikolaos, hub di collegamento di cavi in fibra ottica che collegano Israele, Siria, Libano, Egitto, Turchia, Grecia e Europa continentale. Un altro aspetto che attribuisce alla base di Cipro un alone di inviolabilità è rappresentato da un trattato stipulato tra il governo britannico e quello cipriota, in cui viene stabilito che i rispettivi paesi devono consultarsi e cooperare «per assicurare efficaci operazioni in tema di telecomunicazioni nell'isola di Cipro»[441].

Infine, vi sono le basi del Medio Oriente che risultano cruciali anche per le comunicazioni dirette e provenienti dall'Asia. E' stato il quotidiano inglese The Register a svelare l'esistenza di almeno tre basi segrete gestite dal GCHQ con la connivenza di alcune compagnie telefoniche. Una prima area segreta si troverebbe a Seeb (già segnalata da Snowden), sulla costa settentrionale dell'Oman. Sarebbe stata creata per l'attivazione di un programma dal nome in codice Circuit e si comporrebbe di tre strutture identificabili con i seguenti codici: Timpani (prossima allo stretto di Ormuz); Guitar (a Seeb); Clarinet (vicina al confine con lo Yemen). Se è vero che attualmente il potere di una nazione si misura in funzione della sua capacità di raccogliere e gestire le informazioni a livello mondiale, dovremo forse prepararci a un futuro dove la sorveglianza e l'intrusione dei governi sarà onnipresente e illimitata.

5.4 CAVI SOTTOMARINI E INFRASTRUTTURE CRITICHE: LA LEGISLAZIONE EUROPEA E NAZIONALE

I cavi sottomarini non sono oggetto di uno specifico documento strategico che ne delinei le policy e la legislazione vigente a cui sono sottoposti. Inoltre, i cavi sottomarini sono sottoposti ad una legislazione internazionale per via della loro natura transfrontaliera. Ciò evidenzia come i cavi siano oggetti di molteplici legislazioni e l'assenza di una governance chiara, tanto a livello internazionale quanto nazionale, ha dato luce ad un quadro giuridico particolarmente frammentato. Nel secondo capitolo sono state analizzate le principali fonti di rango internazionale, quali l'UNCLOS, mentre nei prossimi paragrafi ci si soffermerà sulle fonti europee e nazionali. Difatti, i cavi sottomarini vivono

[440] A. Teti, Lo Spionaggio Sottomarini, Gnosis, Marzo 2014.
[441] Ibidem.

una situazione alquanto particolare: da una parte sono un'infrastruttura che si estende per moltissimi paesi e il cui danneggiamento può avere ripercussioni su tutta l'Europa ma dall'altro lato sono anche un'infrastruttura particolarmente rilevante per la sicurezza nazionale che da sempre è la materia di cui i singoli Stati membri sono più gelosi e restii a condividere a livello europeo. Sebbene lo stesso Trattato sull'Unione Europea (TEU) specifica come la sicurezza nazionale sia una responsabilità degli Stati Membri[442], l'Unione Europea ha sempre ritenuto di dover elaborare un sistema di difesa cibernetica a tutela del mercato interno che potesse servire da stimolo ai singoli Stati membri nell'implementazione di misure simili. Ciò in ragione del fatto che l'Unione Europea dispone di mezzi e risorse che le consentono di agire in modo più efficace rispetto ai singoli stati.

5.4.1 L'evoluzione della Strategia Europea in materia di Cybersicurezza

I cavi sottomarini sono una parte fondamentale della sicurezza delle reti e dell'informazione. Tale termine è stato definito dall'Unione Europea per la prima volta nel 2006 come "la capacità di una Rete o di un sistema di informazione di resistere (..) ad eventi imprevisti o atti dolosi che compromettono la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati conservati o trasmessi e dei servizi forniti o accessibili tramite la suddetta Rete o sistema"[443]. Questi sistemi, come i dati che si trasmettono su Internet, possono funzionare grazie ad un "network fisico" rappresentato dalle cosiddette "Infrastrutture Critiche Europee" intese come quelle il cui danneggiamento comporti un impatto su almeno due Stati membri. La fonte comunitaria di riferimento è la Direttiva 2008/114/EC dell'8 dicembre in cui si stabilivano i criteri e le procedure per l'individuazione di tali infrastrutture critiche e dei livelli di sicurezza minimi nella capacità di gestione delle minacce e dei rischi che gli operatori/proprietari di tali asset dovevano rispettare[444]. Il tema della protezione delle infrastrutture critiche aveva assunto particolare rilevanza in termini di sicurezza nazionale a partire dall'attacco alle torri gemelle e aveva portato gli Stati Uniti alla definizione del National Infrastructure Plan (Nipp) ed il G8 all'approvazione dei "G8 Principles for Protecting Critical Information Infrastructures" nel maggio del 2003. Tuttavia, l'impostazione essendo derivata dalle politiche post 9/11, prevedeva un inquadramento della tematica all'interno delle strategie di antiterrorismo. In questo senso, l'Europa è stata in grado di cambiare il paradigma dominante imponendo un approccio del tutto diverso noto come "All-Hazard" che prende le mosse, sia dalla diversa sensibilità e cultura del vecchio continente, ma anche dalla constatazione della fragilità delle Infrastrutture Critiche nei confronti di eventi naturali, accidentali e tecnologici come evidenziato nella

[442] Art. 4, par. 2, TEU. Si veda anche il Considerato 16 del regolamento 2016/679.
[443] Commissione Europea, Una Strategia per una società dell'Informazione Sicura – Dialogo, partenariato, e responsabilizzazione, COM (2006) 656, Bruxelles, pp.3.
[444] Recepita nell'ordinamento italiano con il D.lgs 61/2011.

Comunicazione che istituisce il European Programm on Critical Infrastructure Protection (Epcip)[445]. La Direttiva sulle Infrastrutture Critiche Europee (ECI) presentava diversi problemi dovuti al fatto che si trattava di una tematica afferente alla sicurezza nazionale. Questo è il motivo per cui gli ambiti di applicazione della Direttiva erano esclusivamente quelli dell'energia e dei trasporti. Pertanto, l'infrastruttura dei cavi sottomarini, che al tempo godeva di una minore attenzione rispetto ad oggi, era esclusa dalle Infrastrutture Critiche Europee. Questo si deve anche alla reticenza dei paesi a concedere troppo spazio all'Unione Europea nel legiferare su asset considerati cruciali per la sicurezza nazionale. Un altro elemento limitante era l'approccio multilaterale che prevedeva nel processo di designazione delle infrastrutture critiche europee il coinvolgimento di due o più stati membri (ovvero che un singolo stato non può procedere alla designazione autonoma di una Eci). Inoltre, la Direttiva presentava pochissime indicazioni o obblighi rispetto a come individuare le infrastrutture critiche lasciando notevole libertà agli stati[446]. Ad ogni modo, la direttiva ha colto quello che era l'obiettivo primario, ovvero far crescere l'attenzione sulle problematiche di sicurezza di questi complessi sistemi e sulla necessità di adottare strategie che, con una visione olistica, siano in grado da un lato di migliorare la capacità di cooperazione pubblico privato e dall'altro di favorire la gestione degli elementi di interdipendenza intra- ed inter-settoriali.

Il passo successivo è rappresentato dalla prima Strategia dell'UE in materia di cybersicurezza del 2013 che introduce come necessità strategica per l'Unione la promozione e il rafforzamento della "ciberresilienza". Pertanto, fin da subito l'Unione Europea ha posto il concetto di cyberresilience come pilastro della sua strategia in antitesi all'approccio "militarista" statunitense basato sulla "cybersecurity". Si sottolinea che dall'analisi di diversi documenti europei, quantomeno nell'ambito della sicurezza delle reti e dei sistemi informativi (oggetto delle direttive NIS e NIS2), emerge che il legislatore comunitario usi i termini cibersicurezza e ciberresilienza in modo interscambiabile, identificando pertanto gli stessi ambiti di protezione e gli stessi obiettivi[447]. Parallelamente, vi sono documenti quali il Cyber Resilience Act ed il Cyber Resilience Solidary Act, in cui i due termini possiedono indicatori caratterizzanti[448].

---

[445] Commissione delle Comunità Europee, Comunicazione della Commissione relativa a un programma europeo per la protezione delle infrastrutture critiche - COM(2006) 786 definitivo, 12 dicembre 2006.
[446] R. Setola, M. Tesei, La sicurezza delle infrastrutture critiche tra nuove regole e strategie europee, Sicurezza e Difesa - Europa Atlantica, 12 agosto 2019. Accessibile a https://europaatlantica.it/futuroeuropa/2019/08/la-sicurezza-delle-infrastrutture-critiche-tra-nuove-regole-e-strategie-europee/.

[447] Pier Giorgio Chiara, Raffaella Brighi, La dimensione della "resilienza" nel diritto UE della cybersicurezza, Ragion Pratica, Il Mulino – Rivisteweb,
[448] In via generale, è possibile affermare che Cybersicurezza è maggiormente intesa come la capacità di proteggere i sistemi attraverso controlli preventivi, mentre (cyber) resilienza identifica la capacità di risposta alle sollecitazioni e di adattamento post incidente. Ivi, pp.18.

Nel documento programmatico della Commissione, tale dimensione sembrerebbe sostanziarsi soprattutto nell'ambito della sicurezza delle reti e dell'informazione. Ed è in questo contesto che si sviluppa la proposta per una direttiva recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione, poi Direttiva (UE) 2016/1148 (Direttiva NIS), considerata quale il primo atto giuridico dell'Unione sulla cybersicurezza in senso stretto. La Strategia del 2017, insistendo sull'approccio multi-stakeholder che vede la cybersicurezza quale una sfida sociale comune si sofferma sul rafforzamento dell'ENISA e sulla creazione di un quadro di certificazione europea della cybersicurezza[449].

5.4.2 Codice Europeo delle Comunicazioni Elettroniche (EECC)

Nel dicembre 2018 viene approvato il Codice europeo delle comunicazioni elettroniche (EECC) che è stato trasposto nell'ordinamento italiano[450] solamente tre anni più tardi in seguito all'apertura di una procedura di infrazione da parte della Commissione europea. In Italia, i cavi sottomarini sono oggetto del d. lgs n.207 del 2021[451]. Tuttavia, il contesto normativo europeo risulta variegato. Tradizionalmente, i cavi sottomarini erano posseduti e gestiti da fornitori di servizi e reti di comunicazione elettronica (ECNS)[452] mentre negli ultimi anni i fornitori di contenuti e applicazioni sono diventati i principali proprietari di questa infrastruttura. Quindi, a livello nazionale, i cavi sottomarini sono regolati dal Codice Europeo delle Comunicazioni elettroniche solamente se gli stati ritengono che essi rientrino nella definizione di Electronic Communication Network (ECN) pubblico[453][454] o Electronic Communication Service (ECS)[455] accessibile al pubblico. Nel primo caso ci si riferisce ad un qualsiasi trasmettitore o sistema di trasmissione (oltre alle apparecchiature, al

[449] Allo scopo di garantire elevati standard di sicurezza per prodotti, servizi e processi ICT secondo un approccio di sicurezza by design, sono stati approvati il Cybersecurity Act (Regolamento (UE) 2019/881) ed il Cyber Resilience Act, presentato nel settembre 2022.
[450] D.lgs 8 novembre 2021, n. 207 "*Attuazione della direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio, dell'11 dicembre 2018, che istituisce il Codice europeo delle comunicazioni elettroniche"*
[451] Art.1, comma 1, lettera d, D.lgs n.207 del 2021.
[452] Art. 2 comma 1 lettera s, D.lgs n.207 del 2021, Si intende la "la realizzazione, la gestione, il controllo o la messa a disposizione di tale rete";
[453] Ivi, Art. 2 comma 1 lettera tt, "rete pubblica di comunicazione elettronica: una rete di comunicazione elettronica, utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico, che supporta il trasferimento di informazioni tra i punti terminali di rete;"
[454] Articolo 2(1) dell'EECC, "Sistemi di trasmissione, basati o meno su un'infrastruttura permanente o su una capacità di amministrazione centralizzata, e, se del caso, apparecchiature di commutazione o instradamento e altre risorse, compresi gli elementi di rete non attivi, che consentono la trasmissione di segnali via cavo, radio, ottica o altri mezzi elettromagnetici, comprese le reti satellitari, reti fisse (a commutazione di circuito e a commutazione di pacchetto, compresa Internet) e mobili, sistemi di cavi elettrici, nella misura in cui sono utilizzati per la trasmissione di segnali, reti utilizzate per le trasmissioni radiotelevisive e le reti televisive via cavo, indipendentemente dal tipo di informazioni trasmesse".
[455] Ivi, lettera fff), "servizio di comunicazione elettronica: i servizi, forniti di norma a pagamento su reti di comunicazioni elettroniche, che comprendono, con l'eccezione dei servizi che forniscono contenuti trasmessi utilizzando reti e servizi di comunicazione elettronica o che esercitano un controllo editoriale su tali contenuti".

software e ai dati memorizzati) utilizzato per trasmettere segnali elettronici (compresi suoni, immagini o dati di qualsiasi tipo). Può trattarsi di una rete cablata o wireless, ad esempio una rete di cavi telefonici o una rete di telefonia mobile.[456]. Nel secondo caso si intende un qualsiasi servizio a cui i membri del pubblico possono iscriversi per inviare o ricevere segnali elettronici (compresi suoni, immagini o dati di qualsiasi tipo) – ad esempio, un contratto telefonico o una connessione Internet[457]. Ad ogni modo, l'EECC non fornisce una definizione di ECS disponibile al pubblico e pertanto è tutto rimandato alle legislazioni dei singoli paesi, tra i quali non esiste una definizione comunemente condivisa. Secondo l'Organismo dei regolatori europei delle comunicazioni elettroniche (BEREC), sulla base delle definizioni precedentemente citate, le aziende che installano, producono, riparano o riforniscono sistemi di cavi sottomarini non necessariamente rientrano nella regolamentazione relativa agli Electronic Communication Network and System (ECNS), fatta salva un'analisi specifica delle legislazioni dei singoli paesi[458]. Innanzitutto, la proprietà di una ECN è solo un'indicazione ma non un requisito per determinare la fornitura di tale rete. Inoltre, nel contesto della creazione e della gestione di un determinato sistema di cavi sottomarini, può esistere un'impresa che fornisce ECNS senza essere proprietaria della rete stessa. Dal sondaggio condotto dal BEREC con venti Autorità nazionali di Regolamentazione, è emerso che la maggioranza di esse considererebbe che vi sia una disposizione di ECNS quando un cavo sottomarino con un punto di approdo nel Paese è gestito per fornire capacità agli utenti di quel paese, incluse le imprese che successivamente forniscono ECNS sulla base di tale capacità ad altri utenti del paese[459]. Questo probabilmente comprende i modelli commerciali tradizionali in cui i sistemi di cavi sottomarini sono gestiti da fornitori di ECNS per garantire la capacità internazionale necessaria per supportare le loro attività nazionali al dettaglio e per vendere capacità a terzi all'ingrosso e/o al dettaglio. Questi casi sarebbero probabilmente qualificati come ECN pubblici e/o ECS disponibili al pubblico, in base ai risultati del sondaggio. Tuttavia, negli ultimi anni i cavi sottomarini sono gestiti e posseduti da provider di applicazioni e contenuti che li utilizzano esclusivamente per connettere i loro data centres e quindi per un uso interno. In questo caso non ci si troverebbe dinnanzi ad un ECN pubblico o ECS disponibile al pubblico.

[456] ICO, Key concepts and definitions, Guide to PECR, Accessibile a https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/guide-to-pecr/key-concepts-and-definitions/#publiccommunications.
[457] Ibidem.
[458] BEREC, BoR (23) 214 "Draft BEREC Report on the general authorisation and related frameworks for international submarine connectivity", 7 dicembre 2023, pp. 17.
[459] Ivi, pp.18.

Infine, sempre secondo la ricerca condotta da BEREC, diverse Agenzie di regolamentazione non applicano la legislazione dell'ECNS nel caso in cui le aziende utilizzino i punti di approdo o i cavi per fornire capacità e servizi ad utenti situati esclusivamente al di fuori del territorio nazionale[460]. La legislazione ECNS si applica esclusivamente quando l'utente finale di tale attività si trova sul proprio territorio nazionale.

In conclusione, per determinare se la legislazione relativa agli ECNS si applichi ai cavi sottomarini è necessario analizzare le definizioni nazionali di ECN ed ECS, determinare se tali attività siano definibili come rivolte al pubblico o meno ed infine individuare il ruolo delle singole società ed il modello di business instaurato in relazione a tali sistemi di cavi sottomarini.

5.4.3 Strategia Europea in materia di Cybersicurezza 2020

Nel 2020 la Commissione Europea elabora una strategia pluriennale per la cybersicurezza dell'UE che si pone in linea con i precedenti documenti programmatici ed individua tre settori di intervento: 1) resilienza, sovranità tecnologica e leadership; 2) sviluppo delle capacità operative volte alla prevenzione, alla dissuasione e alla risposta; 3) promozione di un cyberspazio globale e aperto. All'interno del punto 1 si trova la proposta di riformare la Direttiva NIS[461] per "ridurre le incoerenze nel mercato interno allineando i requisiti riguardanti l'ambito di applicazione, la sicurezza e la segnalazione degli incidenti nonché la vigilanza e l'applicazione a livello nazionale e le capacità delle autorità competenti"[462]. In generale si tratta di un documento con un raggio di azione notevolmente ampio, dai prodotti connessi, la catena di approvvigionamento fino alle capacità industriali in ambito cyber, che ha delineato le policy ed iniziative legislative per la cybersicurezza europea degli anni seguenti. In questa direzione si annoverano anche la Direttiva sulla resilienza dei soggetti critici (CER)[463] il cui campo di applicazione è molto simile a quello della NIS II con la differenza che il focus si sposta dalla protezione degli asset fisici alla resilienza dei soggetti che li gestiscono[464]. Oltre alla protezione delle infrastrutture critiche e alla creazione di un sistema di certificazione europeo della cybersicurezza, il documento prevedeva anche la creazione di un "ciberscudo europeo",

[460] Ivi, pp. 19.
[461] La Direttiva UE 2016/1148 sulla sicurezza delle reti e dei sistemi informativi o "Direttiva NIS", uno dei primi tentativi a livello europeo nell'ambito della cyber security, è entrata in vigore nel 2016. In Italia, è stata recepita con il D.lgs. n. 65 del giugno 2018.
[462] Alto Rappresentante dell'Unione per gli Affari Esteri e la Politica di Sicurezza, Comunicazione Congiunta al Parlamento Europeo e al Consiglio - La strategia dell'UE in materia di cibersicurezza per il decennio digitale, 16 Dicembre 2020, Bruxelles, pp. 7.
[463] Commissione Europea, Nuova strategia dell'UE per la cibersciurezza e nuove norme per rendere più resilienti i soggetti critici fisici e digitali, 16 dicembre 2020.
[464] P. Falletta, M. Mensi, Il Diritto del Web, Wolters Kluver, 2021, pp.360.

disegnato inter alia dalla proposta del c.d. Cyber Solidarity Act che, attraverso quadri di cooperazione operativa, intende rafforzare la capacità della UE di prepararsi e gestire gli attacchi su larga scala.

Figura 34:Sandra Schmitz-Berndt, Pier Giorgio Chiara One step ahead: mapping the Italian and German cybersecurity laws against the proposal for a NIS2 directive, 2022.

5.4.4. LA Direttiva NIS 1

La Direttiva NIS, recepita dall'ordinamento italiano con il d.lgs n.65 del 2018, rappresenta un punto fondamentale nel processo di integrazione europeo in quanto ricomprende la sicurezza cibernetica tra le azioni politiche della Commissione Europea. In questo modo termina una fase in cui, in nome della "sicurezza nazionale", gli stati membri avevano potuto godere di enormi margini di manovra. Tuttavia, è bene specificare fin da subito che i cavi sottomarini non erano ricompresi in questa Direttiva. Una scelta sicuramente discutibile vista l'importanza che tale infrastruttura possiede per la Rete ma che fa capire le difficoltà che vi sono state nel trovare un compromesso accettabile da tutti gli stati membri.

L'obiettivo della Direttiva NIS è quello di rafforzare la sicurezza e resilienza informatica all'interno dell'Unione Europea attraverso la predisposizione di standard minimi di pianificazione, scambio di informazioni, cooperazione e obblighi comuni di sicurezza[465]. Pertanto, lo scopo è duplice: da una parte si punta ad una maggiore collaborazione e omogeneità tra gli stati membri[466] e dall'altro si vuole promuovere una cultura della gestione del rischio e di notifica degli incidenti o attacchi digitali tra i soggetti privati. In tal senso, la Direttiva distingue tra gli operatori di servizi essenziali (OSE) e i fornitori di servizi digitali (FSD). Per la realizzazione di questi due obiettivi ciascuno stato membro

[465] Ivi, pp.355.
[466] Questo è lo scopo del Gruppo di Cooperazione" composto da rappresentanti degli stati membri, della commissione e dell'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA).

deve designare: 1) una o più "Autorità competenti NIS" che a loro volta devono individuare gli operatori di servizi essenziali ed i fornitori di servizi digitali; 2) un punto di contatto unico in materia di sicurezza cibernetica per la cooperazione transfrontaliera con le autorità degli altri stati membri; 3) uno o più "*Computer Security Incident Response Team*"(CSIRT) ossia dei gruppi di pronto intervento in caso di attacchi cibernetici[467]. Gli operatori dei servizi essenziali sono scelti dagli stati membri mentre i fornitori di servizi digitali vengono selezionati secondo un'apposita procedura già contenuta nella Direttiva 2015/1535. A differenza della Direttiva del 2008, l'ambito di applicazione è molto più ampio e vi rientrano il settore bancario, le infrastrutture dei mercati finanziari, settore sanitario, fornitura e distribuzione dell'acqua potabile, le infrastrutture digitali, mercato online, motore di ricerca online e cloud computing. Entrambi i soggetti devono individuare le modalità tecniche ed organizzative per la gestione dei rischi e la prevenzione degli incidenti. Per quanto concerne quest'ultimi sono anche stabilite le modalità di notifica agli appositi enti e le relative tempistiche.

La governance della cyber sicurezza italiana predisposta nel recepimento della Direttiva NIS è cambiata in seguito a dei successivi decreti. Innanzitutto, con l'adozione del d.l n. 82 del 2021, convertito in legge n.109/2021, è stata istituita "l'Agenzia per la cybersicurezza nazionale" che è diventata l'autorità nazionale competente NIS ed il punto di contatto unico in materia di sicurezza delle reti e dei sistemi informativi (precedentemente era il DIS) con il compito di monitorare l'applicazione della direttiva. Inoltre, sono state trasferite sotto l'Agenzia anche il CSIRT italiano ed il Centro di Valutazione e Certificazione Nazionale (CVCN)[468].

5.4.5 La revisione della Direttiva NIS e la Direttiva sulla Resilienza dei Soggetti Critici

La Direttiva NIS era riuscita in un compito importantissimo ossia quello di innalzare i livelli minimi di sicurezza in tutti gli Stati membri e di porre al centro dell'agenda dell'Unione Europea la protezione delle reti e dei sistemi. La pandemia ha reso evidente quanto le nostre società non funzionino a compartimenti stagni ma siano sempre più interconnesse e dipendenti tra loro. Inoltre, negli ultimi anni sono emerse nuove minacce che hanno richiesto un aggiornamento della Direttiva NIS I sotto numerosi punti di vista. Tale aggiornamento si collega ad altre iniziative legislative in materia quali il Digital Operational Resilience Act (DORA) che regolamenterà la cybersicurezza del settore bancario, finanziario e assicurativo ed il Cyber Resilience Act (CRA) che mira a stabilire un livello minimo di cybersicurezza per tutti i dispositivi digitali (sia a livello di software sia a livello di

[467] Riunisce le funzioni dei due CERT precedenti (CERT-PA e CERT-N) ed è posto sotto l'autorità della Presidenza del Consiglio dei Ministri.
[468] Istituito con decreto del Ministro dello sviluppo economico del 15 febbraio 2019, in attuazione del D.P.C.M 12 febbraio 2017.

hardware) venduti nel mercato interno dell'UE. Per quanto riguarda i cavi sottomarini, gli atti più rilevanti sono la Direttiva n.2555/2022 entrata in vigore il 17 gennaio 2023[469] e la Direttiva sulla Resilienza dei soggetti critici (CER) che andranno a ricomprendere questa infrastruttura tra quelle oggetto del loro operato.

La direttiva NIS II amplia notevolmente il proprio campo di intervento comprendendovi numerosi settori che erano originariamente esclusi dalla NIS[470] tra cui la stessa infrastruttura dei cavi sottomarini. All'interno della direttiva si sottolinea come "Il mercato interno dipenda più che mai dal funzionamento di Internet" e pertanto è necessario che "le reti pubbliche di comunicazione elettronica, come ad esempio le dorsali Internet o i cavi di comunicazione sottomarini, siano dotate di un'adeguata sicurezza informatica e segnalino gli incidenti in relazione ad esse"[471]. All'interno dello stesso documento, la Commissione specifica come gli stati debbano segnalare eventuali attacchi ai cavi sottomarini al CSIRT nazionale e adottare policy specifiche per la protezione di questa infrastruttura all'interno della strategia per la cybersicurezza nazionale.

Tra i punti focali della direttiva si segnala il superamento della classificazione tra operatori di servizi essenziali e fornitori di servizi digitali propria della NIS 1. L'attuale distinzione è tra "soggetti essenziali" e "soggetti importanti" e si applica a tutte le medie e grandi imprese[472]. Inoltre, gli obblighi di notifica sono stati resi maggiormente stringenti ed immediati: le imprese hanno 24 ore per presentare un rapporto preliminare ed un mese per quello finale più dettagliato. Infine, è stata predisposta una nuova rete di cooperazione operativa denominata "UE – Cyber Crises Liaison Organitation Network" (UE- CyCLONe).

Parallelamente alla NIS II e con scopi analoghi, è stata concepita la Direttiva sulla resilienza dei soggetti critici (CER)[473] che rappresenta l'aggiornamento della Direttiva 2008/114/CE sulle infrastrutture critiche europee. La revisione si è resa necessaria in quanto sono cambiate le tipologie di minacce che riguardano le infrastrutture e sono aumentati i settori considerabili come "critici" per le nostre società. In tal senso, la direttiva amplia il ventaglio dei settori interessati da quello energico

[469] I paesi hanno 21 mesi di tempo per implementarla nel proprio ordinamento.
[470] Tra i soggetti essenziali vi sono: energia, trasporto, settore bancario, settore sanitario, infrastrutture dei mercati finanziari, fabbricazione dei prodotti farmaceutici e dispositivi medici critici, acqua potabile, acque reflue, infrastrutture digitali, pubblica amministrazione e settore spaziale; tra i soggetti importanti: servizi postali e di corriere, settore alimentari, sostanze chimiche, gestione dei rifiuti, computer ed elettronica, veicoli a motore e fornitori di servizi digitali.
[471] Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), Official journal of the European Union, 14 dicembre 2022.
[472] E' presente una deroga per le aziende piccole che operano in settori altamente strategici e possiedono caratteristiche che le rendono di particolare rilievo per la società.
[473] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC

e dei trasporti per farvi ricomprendere il settore bancario, dei mercati finanziari, delle acque reflue e dell'acqua potabile, della salute, delle infrastrutture digitali, della pubblica amministrazione e dello spazio. Lo scopo è quello di uniformare la protezione ed il grado di resilienza di queste infrastrutture in tutti i paesi membri. Lo stesso Consiglio ha sottolineato l'importanza che il Gruppo di collaborazione NIS, con il sostegno della Commissione e dell'ENISA, prepari "orientamenti strategici e metodologie e misure di gestione dei rischi di cibersicurezza secondo un approccio multirischio in relazione ai cavi di comunicazione sottomarini, in previsione dell'entrata in vigore della direttiva NIS2". Ciò a dimostrazione di come i due documenti siano complementari l'uno con l'altro e trattino esplicitamente il tema dei cavi sottomarini. Nello specifico, la direttiva CER impone che ciascuno stato membro individui i soggetti critici (all'interno del settore delle infrastrutture digitali) tra i seguenti tipi di enti: 1) i fornitori di Electronic communication network pubblici (ECN) e gli Electronic Communication Service (ECS) disponibili al pubblico, come definiti dal Codice europeo delle comunicazioni elettroniche (EECC)[474]; 2) Altri tipi, tra cui fornitori di punti di scambio Internet, servizi di cloud computing, servizi di data center e reti di distribuzione di contenuti[475]. Questi soggetti sono da considerarsi "critici" quando: 1)forniscono uno o più servizi essenziali[476]; 2) sono un'infrastruttura critica che è situata, almeno in parte, nel territorio dello stato membro[477]; 3) "Un incidente avrebbe effetti dirompenti sulla fornitura di uno o più servizi essenziali o sulla fornitura di altri servizi essenziali in altri paesi o sulla fornitura di altri servizi essenziali in altri settori pertinenti indicati nell'allegato che dipendono da tale o tali servizi essenziali".

Infine, secondo la direttiva tutti gli stati membri devono adottare delle strategie nazionali per garantire la resilienza dei propri soggetti critici e tali soggetti devono adottare misure tecniche e organizzative adeguate. A livello europeo sono previste esercitazioni comuni per testare la resilienza di questi soggetti critici ed è stato istituito un gruppo di esperti che possa eseguire risk assesment e supporto ai singoli paesi.

5.5. LA LEGISLAZIONE NAZIONALE

5.5.1 Perimetro di Sicurezza Nazionale Cibernetica

Le disposizioni normative analizzate nei paragrafi precedenti trovano la loro fonte giuridica in atti europei. Tuttavia, l'Italia non si è disinteressata dal tema della sicurezza delle infrastrutture critiche e

[474] Articoli 2(1)(5) e 6(1), Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC.
[475] L'elenco completo dei settori, sottosettori e categorie di enti è contenuto nell'Annesso 1 della Direttiva CER.
[476] Sono definiti come "un servizio che è cruciale per il mantenimento delle funzioni vitali della società, delle attività economiche, della salute e della sicurezza pubblica o dell'ambiente". Ivi, Art. 6(2).
[477] Per infrastruttura critica si intende un bene, un impianto, un'attrezzatura, una rete o un sistema, o una parte di un bene, un impianto, un'attrezzatura, di una rete o di un sistema che è necessario per la fornitura di un servizio essenziale".

ha elaborato dei propri strumenti giuridici per aumentare il livello di resilienza e protezione di questi asset. Un passo fondamentale è rappresentato dal decreto legge n.105/2019 (convertito in legge n.133/2019) che ha istituito il Perimetro di Sicurezza Nazionale Cibernetica (PSNC). L'obiettivo primario di questa misura è di fornire una maggiore protezione agli Operatori di Servizi Essenziali (OSE) e ai servizi che da essi dipendono sia dal punto di vista fisico che cibernetico. Pur trattandosi di un elenco secretato, è possibile immaginare che i cavi sottomarini siano ricompresi nel Perimetro Cibernetico dal momento che rispettano tutti i criteri previsti dal D.P.C.M. 131/2020 riguardante i criteri di individuazione di questi soggetti.

Rispetto alla Direttiva NIS, sotto lo "scudo" del Perimetro sono ricompresi ulteriori settori, tra cui la pubblica amministrazione, la difesa, lo spazio e la sicurezza interna. L'elenco dei soggetti facenti parte del Perimetro è escluso dal diritto di accesso e non soggetto a pubblicazione in quanto "tale elenco, considerato nella sua interezza, presenta particolari profili di sensibilità sotto il profilo della sicurezza"[478]. Per tale ragione, l'elenco è pubblicato con un atto amministrativo del Presidente del Consiglio mentre con il D.P.C.M. n.131 del 2020 sono stati individuati i criteri e le procedure di individuazione dei soggetti che possono essere aggiunti al Perimetro e gli obblighi previsti. Secondo il Decreto, si deve trattare di soggetti che svolgono una funzione essenziale e che in tale attività dipendono da reti, sistemi informativi e servizi informativi. Inoltre, l'individuazione deve avvenire sulla base di un criterio di gradualità. La comunicazione ai soggetti di essere stati integrati nel Perimetro viene fatta dal DIS e si hanno sei mesi per adempiere agli obblighi previsti dalla normativa. Il 15 giugno 2021, il Presidente del Consiglio ha comunicato che, in seguito all'estensione dei soggetti inclusi nel Perimetro, i soggetti privati e pubblici coinvolti esercitano 223 funzioni considerate essenziale per lo Stato.

Il Perimetro impone diversi obblighi in capo ai soggetti. Innanzitutto, gli enti devono predisporre un elenco di beni ICT destinati ad essere impiegati sulle reti, i sistemi informativi e per l'espletamento di quelle attività rilevanti ai fini della sicurezza nazionale per un controllo da parte dei Centri di Valutazione. Medesimo obbligo riguarda le procedure di appalto e l'acquisizione di beni oggetto di tali gare in modo tale che il Centro di Valutazione e Certificazione Nazionale (CVCN)[479] possa eseguire dei controlli preliminari e, se necessario, richiedere dei test di hardware e software[480]. Rispetto alla Direttiva NIS I, gli obblighi di notifica al Computer security Incident Response Team

[478] Camera dei Deputati, Sicurezza Cibernetica, Documentazione Parlamentare, Accessibile a https://temi.camera.it/leg18/temi/sicurezza_cybernetica.html.
[479] Tale funzione viene svolta con il supporto dei Centri di Valutazione del Ministero dell'Interno e della Difesa.
[480] Tale disposizione può avere luogo entro 60 giorni dalla comunicazione dell'elenco. D.P.C.M. 30 luglio 2020 n. 131 "Regolamento in materia di Perimetro di sicurezza nazionale cibernetica".

(CSIRT) sono notevolmente più stringenti. La notifica dovrà avvenire entro sei ore dalla scoperta, nei casi di violazione o perdita di confidenzialità o integrità, accesso tramite malware, movimenti laterali o azioni di raccolta ed esfiltrazione di dati[481]. Tale finestra di tempo si riduce ad una sola ora dalla scoperta, nei casi di inibizione delle funzioni di risposta, compromissione dei processi di controllo, disservizio o violazione dei servizi, sistemi o dati[482]. Nel caso in cui gli incidenti abbiano ad oggetto elementi che sono al di fuori del Perimetro, la notifica deve avvenire entro 72 ore. Inoltre, con l'entrata della Direttiva NIS II, gli obblighi di notifica aumenteranno e sarà necessario creare un quadro maggiormente armonizzato per evitare che vi siano inutili sovrapposizioni di funzioni e rapporti.

5.5.2 Il Golden Power ed il caso Sparkle

Perr ultimare l'analisi del quadro giuridico nazionale a cui sono sottoposti i cavi sottomarini, è necessario trattare uno degli strumenti più rilevanti ed incisivi del nostro panorama normativo, il Golden Power. Esso è stato oggetto di una lunga e corposa revisione nel corso degli anni che ha portato la Commissione Europea a chiudere la procedura di infrazione nei confronti dell'Italia[483]. Difatti, l'istituto prende origine dalla Golden Share inglese o Action Spècifique francese che permettevano allo Stato di opporsi all'acquisizione di partecipazioni rilevanti di qualsiasi tipo, anche intra UE, tramite delle apposite disposizioni contenute negli statuti delle principali società di diritto italiano ai sensi del decreto l. n. 332 del 1994 (convertito in l. n. 474 del 1994). Il decreto imponeva che negli statuti delle società operanti nel settore dell'energia, dei trasporti, delle comunicazioni e della difesa fosse inserita una clausola per la quale, prima della perdita di controllo della società, il Ministero delle Finanze avrebbe assunto una serie di poteri speciali che gli garantivano di porre veti e condizioni sulle decisioni relative all'azienda. Nelle Comunicazioni della Commissione del 19 luglio 1997, veniva sottolineato come i poteri attribuiti dalla Golden Share potessero rappresentare una lesione della libertà di stabilimento e di circolazione dei capitali garantiti dai trattati europei in quanto l'esercizio di tali poteri sarebbe consentito solamente qualora si fondasse su "criteri obiettivi, stabili e resi pubblici" e giustificato da "motivi imperiosi di interesse generale". Per mezzo del decreto-legge n. 21 del 2012 sono stati ridefiniti, anche mediante il rinvio ad atti di normazione secondaria (DPCM), l'ambito oggettivo e soggettivo, la tipologia, le condizioni e le procedure di esercizio da parte dello Stato (in particolare, del Governo) dei suddetti poteri speciali.

Una prima importante novità è rappresentata dal fatto che lo Stato può esercitare questi poteri nei confronti di tutte le società che svolgono attività considerate strategiche e non solo nei confronti delle

[481] D.P.C.M n.81 del 14 aprile 2021, Allegato A, tabella 1.
[482] D.P.C.M n.81 del 2021, Allegato A, tabella 2.

[483] Procedura di infrazione n.2009/2555. Lo stato italiano venne deferito alla Corte il 24 novembre 2012.

società privatizzate o in mano pubblica. Rispetto ai settori di intervento, la Commissione ha ammesso un regime particolare per gli investitori di un altro Stato membro qualora esso sia giustificato da motivi di ordine pubblico, di pubblica sicurezza e di sanità pubblica purché, conformemente alla giurisprudenza della Corte di giustizia, sia esclusa qualsiasi interpretazione che poggi su considerazioni di ordine economico. Questo elemento risulta di particolare rilevanza dal momento che diversi dossier su cui è intervenuto lo Stato negli ultimi anni hanno riguardato aziende di stati membri. Basti pensare al tentativo di acquisto di Microtecnica da parte dell'azienda francese Safran[484]. Con una disciplina di fonte secondaria sono stati stabiliti gli ambiti soggettivi e oggettivi e le procedure di applicazione del Golden Power per quanto concerne i settori della difesa, della sicurezza nazionale (d.P.R. n.35/2014) e dell'energia, dei trasporti e delle comunicazioni. Nel primo caso è necessaria la sussistenza di una minaccia di grave pregiudizio per gli interessi essenziali della difesa e della sicurezza nazionale**.** In tal caso, l'esecutivo può: imporre specifiche condizioni all'acquisto di partecipazioni in imprese strategiche nel settore della difesa e della sicurezza; porre il veto all'adozione di delibere relative ad operazioni straordinarie o di particolare rilevanza, ivi incluse le modifiche di clausole statutarie eventualmente adottate in materia di limiti al diritto di voto o al possesso azionario; opporsi all'acquisto di partecipazioni, ove l'acquirente arrivi a detenere un livello della partecipazione al capitale in grado di compromettere gli interessi della difesa e della sicurezza nazionale.

Gli obblighi di notifica sono estesi alle delibere, atti o operazioni aventi ad oggetto il mutamento dell'oggetto sociale, lo scioglimento della società, la modifica di clausole statutarie riguardanti l'introduzione di limiti al diritto di voto o al possesso azionario. Il veto alle delibere, atti o operazioni può essere espresso qualora essi diano luogo a una situazione eccezionale, non disciplinata dalla normativa – nazionale ed europea - di settore, di minaccia di grave pregiudizio per gli interessi pubblici relativi alla sicurezza e al funzionamento delle reti e degli impianti e alla continuità degli approvvigionamenti, ivi compresi le reti e gli impianti necessari ad assicurare l'approvvigionamento minimo e l'operatività dei servizi pubblici essenziali. Nel computo della partecipazione rilevante ai fini dell'acquisto si tiene conto della partecipazione detenuta da terzi con cui l'acquirente ha stipulato patti parasociali. Anche per le violazioni di cui al presente articolo è prevista la sanzione della nullità degli atti. Qualora tali soggetti non adempiessero agli obblighi di notifica citati, è stata introdotta una sanziona amministrativa pecuniaria[485]. Inoltre, con il medesimo decreto, è stato individuato un criterio specifico cui il Governo deve attenersi nell'esercizio dei poteri speciali, con riferimento a

[484] R. Scala, L'Italia attiva il Golden Power per bloccare la Francia, IARI, 2 dicembre 2023. Accessibile a https://iari.site/2023/12/02/litalia-attiva-il-golden-power-per-bloccare-la-francia/
[485] Art. 14 del decreto-legge n. 148 del 2016

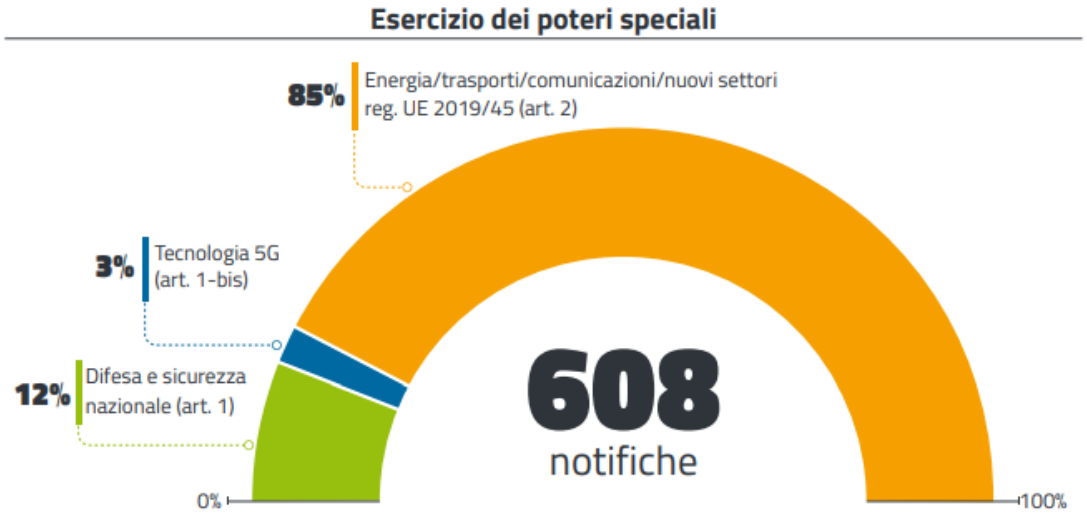
quelle operazioni di acquisto da parte di soggetti extra UE di società che detengono attivi strategici nel settore energetico, dei trasporti e delle comunicazioni, ove l'acquisto di partecipazioni determini l'insediamento stabile dell'acquirente. In tali ipotesi il Governo deve valutare, oltre alla minaccia di grave pregiudizio agli interessi pubblici relativi alla sicurezza e al funzionamento delle reti e degli impianti e alla continuità degli approvvigionamenti, anche il pericolo per la sicurezza o per l'ordine pubblico.

Le ultime modifiche a questa normativa sono avvenute durante il periodo pandemico in quanto vi era la preoccupazione che la Cina potesse approfittare del momento di debolezza del sistema economico italiano per acquisire partecipazioni in asset strategici. Questa preoccupazione è stata condivisa da diversi paesi europei e ha trovato una sua applicazione nel regolamento europeo n. 459 del 2019 sul controllo degli investimenti esteri. Il governo italiano ha convogliato le considerazioni del COPASIR del 25 marzo 2020 e della stessa Commissione Europea[486] all'interno del decreto legge "Liquidità" con il quale si amplia notevolmente il ventaglio di settori coperti da Golden Power facendovi rientrare quello agroalimentare, quello finanziario, creditizio, assicurativo, sanitario, le infrastrutture aereospaziali, elettorali, la robotica, i semiconduttori, le infrastrutture sensibili nonché gli investimenti in acquisto di terreni e immobili fondamentali per l'utilizzo di tali infrastrutture ed anche i media ed il settore dell'informazione. La normativa si applica ai soggetti UE solamente quando l'acquisto di partecipazione risulti rilevante per il controllo della società. Per i soggetti extra UE, è previsto l'obbligo di notifica solamente nella fattispecie in cui l'acquisto di partecipazione attribuisce un diritto di voto o di capitale superiore al 10% all'acquirente. Le disposizioni del decreto "Liquidità" avevano una durata prestabilita fino al 31 dicembre 2020 ma sono state rinnovate e ampliate dal D.L 21/2022 (cd. "Ucraina Bis"). Ad esempio, è stato poi ampliato il campo di applicazione oggettivo della disciplina, mediante l'inclusione, tra le operazioni soggette all'obbligo di notifica, dei cc.dd. "greenfield investiments", ossia gli investimenti che si realizzano non tramite l'acquisizione di partecipazioni in imprese già esistenti, ma attraverso la costituzione ex novo di un soggetto economico. Sono stati infine introdotti meccanismi di semplificazione procedurale, come quello della "prenotifica", che permette di fornire agli investitori una valutazione preliminare sulla applicabilità o meno della disciplina Golden Power alle singole operazioni prospettate, nonché sulla loro autorizzabilità.

Negli ultimi anni è aumentato notevolmente l'utilizzo di questo strumento. Basti pensare che nel 2022 si è assistito ad un aumento del 22% delle operazioni sottoposte allo scrutinio dei poteri speciali per

[486] Raccomandazione (UE) 2019/534 della Commissione del 26 marzo 2019, Cibersicurezza delle reti 5G. Accessibile a https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32019H0534

un totale di 608 notifiche[487] (nel 2014, furono soltanto otto le notifiche). Sebbene la revisione della normativa sia stata fatta in un'ottica difensiva rispetto alla Cina, è da sottolineare come siano aumentati notevolmente i casi in cui erano coinvolte aziende di paesi europei. Da ultimo, il governo italiano ha invocato i poteri speciali sulla vendita da parte di TIM della sua rete di infrastrutture fisiche che fa riferimento a NetCo per un valore di 18,8 miliardi. L'operazione coinvolge il Ministero dell'Economia che possiede il 10% delle azioni di TIM tramite CDP e l'acquirente americano Kohlberg Kravis Roberts & Co (KKR). La trattativa è stata approvata con una serie di prescrizioni da parte del governo il 17 gennaio 2024. Tuttavia, nell'accordo iniziale non era ricompresa Sparkle, anch'essa controllata da Tim, che è uno dei principali fornitori di cavi sottomarini del Mediterraneo ed è coinvolto in numerosi progetti di carattere globale. Difatti, nella trasformazione di Tim in società di servizi non dovrebbe esserci posto per una società come Sparkle basata sul possesso e costruzione di infrastrutture. Per queste ragioni, il MEF è intervenuto con una proposta di rilevamento del 100% della società per un valore di 600 milioni (più 150 milioni di riconoscimenti addizionali eventuali, earn out). Inoltre, il MEF sembrerebbe essere pronto ad alzare la sua valutazione qualora Tim mantenesse una quota minoritaria per un determinato arco temporale e supportasse la realizzazione del piano strategico. Si tratta di un dossier strategico per l'Italia che non può permettersi di perdere il suo principale player di cavi sottomarini se vuole affermarsi come hub energetico e digitale del Mediterraneo.



Il sabotaggio dei gasdotti Nord Stream e il successivo picco di attività da parte di imbarcazioni russe in prossimità di infrastrutture critiche informatizzate, compresi cavi, condutture e parchi eolici nel

[487] Nel 2021 erano 496, nel 2020 sono state 342 e nel 2019 solamente 83. Il Post, Cos'è il "golden power", 19 giugno 2023. Accessibile a https://www.ilpost.it/2023/06/19/golden-power-pirelli/.

Mare del Nord, hanno messo in evidenza, per molti versi, le sfide da affrontare per proteggere efficacemente tali beni semplicemente rafforzando la presenza navale convenzionale nelle aree interessate. Innanzitutto, le reti UCI sono in continua espansione e già così estese che è praticamente impossibile garantire la presenza navale persistente necessaria per monitorarle efficacemente per lunghi periodi di tempo. Per questo motivo, il futuro della protezione di queste infrastrutture risiede nell'utilizzo di dati provenienti da diverse fonti come il Sistema di Identificazione Automatica (AIS)[488] i sensori satellitari ed i radar terrestri e subacquei che possono essere montati direttamente sui cavi sottomarini[489].

Nonostante il fatto che l'Europa sia considerata dagli stakeholder privati come un punto di riferimento globale per le questioni normative, la realizzazione di sistemi di cavi sottomarini dipende dall'adempimento di un numero significativo di procedure amministrative nazionali di autorizzazione in campi che esulano dal settore ECNS, tra cui la tutela dell'ambiente, protezione del patrimonio culturale, la pianificazione e la gestione delle risorse marittime e la pianificazione e la gestione urbana e del territorio, che comportano una durata media complessiva che può superare un anno. Inoltre, anche se alcuni paesi hanno già creato punti di contatto unici e/o meccanismi di cooperazione nazionale tra le autorità competenti, questo non è ancora generalizzato. Basti pensare che a livello europeo manca un punto di contatto unico e la governance risulta particolarmente frammentata sia dal punto di vista della gestione degli incidenti che dell'elaborazione normativa e di politiche pubbliche.

Infine, le rivelazioni di Snowden hanno aperto un vaso di pandora dimostrando quanto le nostre comunicazioni fossero poco protette. A più di dieci anni di distanza non è possibile affermare che operazioni di quel tipo non siano più attuabili. Anzi, gli sviluppi tecnologici rendono possibile lo spionaggio dei cavi sottomarini senza il bene placito delle compagnie telefoniche. Sul piano normativo, l'Europa vuole affermarsi come garante della privacy dei cittadini e hub tecnologico ma la paura degli stati membri di perdere controllo su tematiche che riguardano così da vicino la sicurezza nazionale ha reso molto complicato il processo di elaborazione di una strategia comune. La buona notizia è che i cavi sottomarini sono diventati un tema centrale dell'agenda europea in materia di cybersicurezza e di sicurezza comune. Sebbene ancora manchi un documento strategico che detti la

[488] L'AIS è un sistema di tracciamento per le navi di superficie. Le linee guida dell'Organizzazione Marittima Internazionale (OIM) stabiliscono che le navi non possono mai spegnere l'AIS quando sono in navigazione o all'ancora. Si veda: NATO Shipping Centre, "AIS (Automatic Identification System) Overview", in NSC News, 22 ottobre 2021, https://shipping. nato.int/nsc/operations/news/2021/ais-automatic-identification-systemoverview.
[489] Op. Cit. M. Battaglia, Difesa Underwater, Buttita presenta le nuove tecnologie sottomarine.

linea da seguire, la normativa più recente ha incluso i cavi sottomarini e questo rappresenta un primo importantissimo passo verso la sicurezza delle nostre comunicazioni.

CONCLUSIONI

L'analisi condotta ha messo in luce come i cavi sottomarini siano un'infrastruttura tanto strategica quanto vulnerabile. Le nostre attività quotidiane dipendono da sottilissimi fili di vetro poggiati sui fondali marini. Il sistema economico globale si regge sulla velocità di trasmissione dei dati garantita da questa infrastruttura. Le grandi potenze ne sono consapevoli e stanno adottando differenti strategie per poter controllare questo settore: la Russia, consapevole di non essere una potenza economica, si vuole affermare come la principale minaccia militare tramite la propria flotta subacquea. La Cina mira al controllo del settore mediante una guerra commerciale con gli Stati Uniti. Le infrastrutture sono il mezzo con il quale la Cina si proietta nei paesi in via di sviluppo ed il controllo delle comunicazioni è vitale per una grande potenza. Gli Stati Uniti sono la potenza egemone che ha plasmato internet a sua immagine e somiglianza e ne ha fatto un grande megafono. Tuttavia, negli ultimi dieci anni qualcosa è cambiato, sia perché le grandi aziende tech non rispondono sempre alle volontà del governo e sia perché gli scandali sullo spionaggio statunitense ne hanno fortemente indebolito l'immagine all'estero. Pertanto, vi sono due domande alle quali bisognerà rispondere nel minor tempo possibile: che ruolo possono avere Europa ed Italia? Come possiamo proteggere questa infrastruttura per evitare di cadere in un blackout senza possibilità di riavvio del sistema?

Nel quinto capitolo si è analizzato il ruolo che l'Italia dovrebbe ricoprire nell'ecosistema dei cavi sottomarini per via della sua posizione geografica. Basti pensare, che dopo gli Stati Uniti siamo il paese che possiede il betweenness centrality score più alto[490][491]. In una rete di telecomunicazioni, un nodo con una betweenness centrality più alta avrà un maggiore controllo sulla rete, perché attraverso di esso passeranno più informazioni. Questo rende l'Italia un paese molto importante per il sistema delle comunicazioni globali e ci obbliga a rafforzare il grado di resilienza della nostra infrastruttura. Inoltre, le infrastrutture sono uno strumento di cooperazione internazionale, specialmente nelle relazioni bilaterali come dimostrato dal rapporto che si è instaurato nel corso degli anni tra Italia e Libia. La Cina ne ha fatto il marchio di fabbrica della propria strategia. In tal senso, le relazioni con i paesi africani andrebbero modulate sul supporto nella costruzione di questo tipo di infrastrutture che

[490] Margaret Ross, Understanding Interconnectivity of the Global Undersea Cable Communications Infrastructure and Its Implications for International Cyber Security, 34 SAIS REV. International 'Affairs. 141, 2014.
[491] Ibidem, pp.10. Un attore ha un'elevata betweenness nella misura in cui si trova
si trova sul percorso più breve tra altre coppie di attori della rete.

possono garantire maggiore stabilità economica e rapporti più stretti con l'altra sponda del Mediterraneo. Perché ciò sia possibile, l'Italia deve costruirsi una propria autonomia rispetto all'ingerenza degli Stati Uniti che in passato hanno utilizzato le nostre landing station per operazioni di spionaggio. La sicurezza delle comunicazioni è la condizione necessaria ma non sufficiente per poter instaurare questo tipo di strategia. La sicurezza del sistema passa per una diversificazione dei punti di approdo, una maggiore protezione di quest'ultimi, un rafforzamento della flotta di riparazione dei cavi che oggi è di natura prettamente privata ed un controllo costante dei nostri mari. Queste problematiche dovranno essere affrontate in un documento strategico e trovare applicazione concreta anche nelle licenze che lo stato italiano approva nei confronti dei privati che vogliono costruire cavi nel nostro paese. Si è sottolineato più volte il grado di interconnessione ed interdipendenza che caratterizza questo settore e ciò implica che le strategie nazionali possono funzionare solo se integrate in un quadro più ampio.

Pertanto, l'Italia può e deve affermarsi come un importante hub digitale ma è solo tramite l'Unione Europea che sarà possibile incidere sui quesiti che ci si è posti ad inizio paragrafo. Tuttavia, l'Europa deve risolvere diverse questioni interne che attualmente le impediscono di predisporre una strategia unica. Cùome più volte ribadito in questo elaborato, il settore in questione ha importanti ripercussioni sul piano della sicurezza nazionale motivo per il quale i paesi membri tendono a voler mantenere un particolare controllo. Un controllo motivato anche dall'interesse dei singoli paesi di sponsorizzare maggiormente le proprie aziende nazionali ed i propri progetti in modo tale da poter costruire relazioni più strette con paesi esteri. Si tratta di una competizione interna all'Unione dalla quale nessuno potrà uscirne realmente come vincitore. Per elaborare una politica comune sarà necessario derimere le numerose controversie riguardanti le ZEE nel Mediterraneo Orientale ed elaborare un dispositivo militare europeo che consenta un margine di autonomia rispetto alla NATO e che permetta di proteggere le proprie infrastrutture critiche.

Nell'ottica di un approccio condiviso, Bruxelles ha a disposizione tre possibili approcci: quello cooperativo, quello competitivo e quello militare. Innanzitutto, è da scartare aprioristicamente una risposta isolazionista sulla falsa riga del programma "Clean Network" presentato dall'amministrazione Trump nel 2019 che distingueva tra cavi "puliti" e cavi pericolosi (in quanto possedevano punti di approdo in Cina) con lo scopo di veicolare i dati dei propri cittadini esclusivamente su determinati cavi sottomarini. Si tratta di un approccio impossibile da eseguire in quanto internet non è compartimentalizzabile ed oltretutto sarebbe anche controproducente perché

consentirebbe alla Cina di "perseguire uno stack tecnologico separato, dotato di un proprio processo di definizione degli standard che includa un sottoinsieme di paesi BRI/DSR"[492].

L'APPROCCIO COOPERATIVO

Pertanto, l'Unione Europea dovrebbe innanzitutto scegliere una risposta cooperativa il cui scopo ultimo dovrebbe essere quello di redigere un trattato internazionale apposito sui cavi sottomarini. Un accordo a livello internazionale potrebbe richiedere molto tempo e non vedere mai la luce motivo per il quale è necessario trovare un accordo almeno con i paesi alleati. In alternativa alla via istituzionale, si potrebbe trattare direttamente con l'ICPC che potrebbe vincolare la partecipazione al suo forum al rispetto di determinate regole. Al netto della modalità, ciò che conta maggiormente è il contenuto della risposta cooperativa. Innanzitutto, è fondamentale promuovere la creazione di una governance per i cavi sottomarini all'interno delle Nazioni Unite. Un secondo passo sarebbe quello di stabilire delle zone di protezione internazionale attorno alle rotte dei cavi sottomarini nell'alto mare e nelle ZEE. In questo modo, si diminuirebbero fortemente i danni accidentali e sarebbe più semplice rintracciare eventuali attività sospette. Il trattato sarebbe necessario anche per aggiornare diverse norme contenute nell'UNCLOS che ad oggi appaiono anacronistiche o non sono proprio oggetto del trattato tra cui stabilire se i cavi sottomarini sono un obiettivo di guerra legittimo. Un tema sul quale si potrebbe trovare un accordo internazionale, soprattutto grazie alla pressione delle aziende, è quello delle navi da riparazione e delle relative licenze. Difatti, vi sono paesi che risultano particolarmente tardivi nell'approvare le richieste di ingresso delle navi specializzate nelle acque territoriali con conseguenze molto gravi sulla connettività mondiale. Questo fenomeno è sia dovuto all'inefficienza burocratica di alcuni paesi ma allo stesso tempo non è da escludere che vi sia la volontà di rallentare queste operazioni per creare danni economici a paesi rivali. Una proposta interessante sarebbe quella di assegnare a tutte queste navi specializzate lo status di "passaggio innocuo" ed eliminare ogni tipo di tasse o licenza. Al netto delle singole proposte, l'approccio cooperativo risulta in linea con la cultura europea e la sua proiezione esterna come soggetto regolatore e protettore dei dati. A differenza degli Stati Uniti, l'Europa vanta una reputazione senz'altro migliore che le consente di proporsi come interlocutore nei confronti di diversi paesi in via di sviluppo. Come suggerito da Bueger e Liebetrau, le infrastrutture critiche possono essere utilizzate in politiche di state building[493] e ciò dovrebbe essere preso in debita considerazione dall'UE. Questi diversi elementi dovrebbero comporre un piano strategico in modo analogo alla Digital Silk Road cinese. (

[492] Greene, Robert, Paul Triolo, "Will China Control the Global Internet Via Its Digital Silk Road?" Carnegie Endowment for International Peace. Maggio 8, 2020.
[493] Op.Cit, Bueger Liebetrau, Protecting hidden infrastructure: The security politics of the global submarine data cable network.

APPROCCIO COMPETITIVO

La strategia europea deve muoversi su due versanti. Il primo è quello descritto dall'approccio cooperativo con il quale l'Europa deve garantirsi soprattutto un sostegno politico a livello internazionale. Tuttavia, questo da solo non basta per affermarsi come attore internazionale. Per contrastare l'espansionismo cinese ed il predominio statunitense è necessario imporsi sul piano commerciale. In questo senso, l'Unione Europea deve elaborare una vera e propria politica industriale che consenta alle sue aziende di proporsi non solo come le più sicure ma anche le più vantaggiose da un punto di vista economico. Il successo della DSR risiede principalmente nelle tariffe che le aziende cinesi possono offrire ai paesi in via di sviluppo. Si tratta soprattutto di una guerra commerciale e tecnologica. Bruxelles ha mosso i primi passi tramite l'adozione del Connectivity Europe Facility (CEF2)[494] le cui risorse sono assolutamente insufficienti per poter competere con le grandi potenze. Lo scopo è duplice: da una parte supportare le proprie aziende in modo tale da poter espandere il proprio raggio d'azione e dall'altra diminuire la dipendenza da cavi che vedono la presenza di aziende cinesi. Questo approccio garantirebbe una maggiore ridondanza ai paesi europei e allo stesso tempo consentirebbe all'Europa di affermarsi come potenza commerciale nel continente africano.

APPROCCIO MILITARE

La protezione di queste infrastrutture deve essere l'elemento che circonda tutta la strategia europea in materia di cavi sottomarini. Da questo punto di vista, è necessario un cambio di paradigma. In un mondo sempre più interconnesso, anche la sicurezza nazionale non è più una tematica affrontabile paese per paese ed i cavi sottomarini ne sono la perfetta rappresentazione. Un attacco digitale nei confronti di una stazione di approdo spagnola potrebbe rapidamente diffondersi come un virus tramite i cavi sottomarini in tutti gli altri paesi, compresi quelli che non possiedono uno sbocco marittimo. Dal terzo capitolo di questo lavoro è emerso come il sabotaggio della connettività europea risulti quasi impossibile ma lo stesso non si può dire per le attività di spionaggio nei confronti di questa infrastruttura. Pur trattandosi di materiale classificato, è ragionevole pensare che operazioni di questo tipo siano state svolte nei nostri mari. Pertanto, risulta fondamentale predisporre un dispositivo militare a guida europea incaricato esclusivamente della protezione delle infrastrutture critiche situate nel Mediterraneo. Tale approccio prevede anche che l'industria militare e civile si investa su sensori di rilevamento da poter posizionare sui cavi stessi e sulla costruzione di droni subacquei che consentano di avere una maggiore consapevolezza dei propri fondali marini. In tal senso, le marine europee dovrebbero organizzare delle esercitazioni comuni che abbiano ad oggetto la guerra anti

[494] Meccanismo per collegare l'Europa — Meccanismo per collegare l'Europa digitale, Commissione Europea, 22 settembre 2021.Accessibile a https://digital-strategy.ec.europa.eu/it/activities/cef-digital.

sommergibile e subacquea. In questa direzione sembra muoversi anche la NATO tramite la creazione di un apposito Centro marittimo per la sicurezza delle infrastrutture critiche sottomarine che sorgerà nel Comando marittimo alleato di Londra. La difesa comune sembra ancora molto lontana ma la protezione delle infrastrutture critiche potrebbe essere un valido discorso su cui far leva per imporre una maggiore collaborazione e procedere verso un concetto di sicurezza nazionale europea. Protezione dei dati, alti standard tecnologici, collaborazione internazionale e regionale, costruzione di una propria autonomia strategica. Se l'Europa vuole sedere al tavolo dei "grandi" non deve avere paura di giocare le proprie carte.

Il tema delle infrastrutture critiche mette in luce tutte le difficoltà dell'Italia e dell'Europa. La mancanza di una propria consapevolezza interna, di una direttrice che accomuni le scelte strategiche, di quelli che sono gli interessi nazionali. Il risultato è che l'Europa non riesce a proiettarsi esternamente, ad uscire dal suo guscio e presentarsi come un attore valido perché non se ne conoscono le intenzioni. Gli stati membri sono ancora legati a logiche conflittuali interne e l'Italia si trova spesso in una situazione di mediazione o di limbo. Un paese che per storia e geografia dovrebbe possedere una proiezione marittima e che invece non sa dove deve andare.

Una cosa è certa, la prossima guerra passerà per i cavi sottomarini e potrebbe avere impatti devastanti sulla società. E' arrivato il momento di prevedere un piano B.

Riferimenti

A. Gross, A. Heal, C. Campbell et al. «How the US is pusching China out of the Internet's plumbing.» *Financial Times.* 13 giugno 2023. a https://ig.ft.com/subsea-cables/.

al., L. Carter et. *Submarine Cables and the Oceans - Connecting the World.* Cambridge: UNEP-WCMC Biodiversity Series no. 31, 2009.

Burdette, , Princeton University, JPIA, 5 Maggio 2021. «Leveraging Submarine Cables for Political Gain: U.S. Responses to Chinese Strategy.» *Journal of Public and International Affairs (JPIA)*, 5 maggio 2021.

C. Bueger, T. Liebetrau. «Christian Bueger & Tobias Liebetrau (2021) Protecting hidden infrastructure: The security politics of the global submarine data cable network.» *Contemporary Security Policy, 42:3*, 2021: 391-413.

C. Bueger, T. Liebetrau, J. Franken. *Security Threats to Undersea Communications Cables and Infrastructure: Consequences for the EU* . Sottocomissione del Parlamento Europeo per la Sicurezza e la Difesa, 2022.

C. Gerlach, R. Seitz. *Economic Impact of Submarine Cable Disruptions.* APEC Policy Support Unit, 2012.

Clark, B. «Undersea Cables and the Future of Submarine Competition.» *Bulletin of the Atomic Scientists 72(4):1-4*, 15 giugno 2016.

D. Burnett, T. Davenport, R. Beckman. *Submarine cables : the handbook of law and policy.* Leiden: Martinus Nijhoff;, 2014.

D. Guilfoyle, T Paige, R. McLaughlin. «THE FINAL FRONTIER OF CYBERSPACE: THE SEABED BEYOND NATIONAL JURISDICTION AND THE PROTECTION OF SUBMARINE CABLES.» *International e Comparative Law Quarterly, Volume 71, Issue 3*, 2022: 657-696.

D. Reverdy, I. Skenderoski. *Submarine Cables: Structuring and Financing Options. .* Salience Consulting White Paper, 2015.

Davenport, T. «"Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis".» *Catholic University Journal of Law and Technology 24, no. 1*, Autunno 2015: 57-110.

Deeks, A. «An International Legal Framework for Surveillance.» *Virginia Jpurnal of International Law*, 2015: 293-378.

Fraizier, K. «Policy Proposals for the United States to Protect the Undersea Cable System.» *Journal of Law, Technology & the Internet* 13, n. 1 (2021-2022): 37.

G. Bafoutsou, M. Papaphilippou, M. Dekker. *Submarine Cables, What is at Stake.* Policy Paper, ENISA, 2023.

Green, M. «The Submarine Cable Industry: How Does it Work?» In *Submarine Cables: the Handbook of Law and Policy*, di D. Burnett T. Davenport. 2013.

Hayashi, Moritaka. «Military and intelligence gathering activities in the EEZ: definition of key terms.» *MarinePolicy*, 2015: 123-137.

Hillman, J. *Securing the Subsea Network: A Primer for Policymakers.* CSIS, 2021.

Jill C. Gallagher, Nicole T. Carter. *Protection of Undersea Telecommunication Cables: Issues for Congress.* Congressional Research Service, agosto 2023.

Kavanagh, C. *Wading Murky Waters: Subsea Communications Cables and Responsible State Behaviour.* Geneva: UNIDIR, 2023.

Kaye, S. «The Protection of Platforms, Pipelines and Submarine Cables under Australian and New Zealand Law.» In *Maritime Security: International Law and Policy Perspectives from Australia and New Zealand*, di J. Mossop, D. Rothwell N. Klein, 186-201. Routledge, 2010.

Khazan, Olga. «The Creepy Long-Standing Practice of Undersea Cable Tapping.» *The Atlantic*, 13 Luglio 2013.

Kulesza, Balleste. *Cybersecurity and Human Rights in the Age of Cyberveillance.* New York: Rowman & Littlefield Pub Inc, 2015.

L. Lo Porto, M. Baticci. *I cavi sottomarini come infrastruttura critica - rischi, trend e opportunità per l'Italia.* Roma: Aware, 2022.

Liao, Xuexia. «Protection of Submarine Cables against Acts of Terrorism.» *Ocean Yearbook*, 2019: 456-486.

M. Colombo, F. Solfrini, A. Varvelli. *Network effects: Europe's digital sovereignty in the Mediterranean.* Policy Brief, European Council on Foreign Relations, 2021.

M. Marconi, Sellari, D. Aprea et al. *Civiltà del mare - Geopolitica, strategia, interessi nel mondo subacqueo. Il ruolo dell'Italia.* Fondazione Leonardo, Marina Militare Italiana, 2023.

Masiello, A. *Sicurezza delle reti e infrastrutture critiche nel Mediterraneo, Italia Strategic Governance.* Aliseo, 2022.

Matis, M. *The Protection of Undersea Cables: A Global Security Threat.* United States Army War College, 2012.

N. Gelvanovska, M. Rogy, and Carlo Maria Rossotto. *Broadband Networks in the Middle East and North Africa Accelerating High-Speed Internet Access.* Banca Mondiale, 2014.

PWC. *Study to Monitor Connectivity – Connecting the Eu to its partners through submarine cables.* Commissione Europea, 2022.

Renault, L. «The Protection of Submarine Telegraphs and the Paris Conference.» Merzbach and Falk, 1884.

Sechrist, M. *Cyberspace in Deep Water: Protecting Undersea Communication Cables.* Harward Kennedy School, 2013.

Sechrist, M. *New Threats, Old Technology – Vulnerabilities in Undersea Communications Cable Network Management Systems, .* Harward Kennedt School - Belfer Center, 2012.

Sherman, Justin. *Cyber Defense Across the Ocean Floor - the Geopolitics of Submarine cable security.* Atlantic Council - Scowcroft Center for Sytrategy and Security, 2021.

Shvets, D. *The International Legal Regime of Submarine Cables: a Global Public Interest Regime.* Barcellona: Universitat Pompeu Fabra Barcelona, 2020.

Submarine Cable System Market. Precedence Research, 2023.

Sunak, R. *Undersea Cables: Indispensable, Insecure.* Policy Exchange, 2017.

Sydney, Brooke, Pleasic. *Securing Subsea Cable Critical Infrastructure, Holes in the Governing Legal Framework in the United States and Internationally.* Seton Hall University, 2024.

T.Davenport. «Submarine cables, cybersecurity and international law: an intersectional analysis.» *Catholic University Journal of Law and Technology* , 2015: 57-110.

Teti, A. «Spionaggio Sottomarino.» *GNOSIS - Rivista italiana di Intelligence*, 2014.

The United Nations Convention on the Law of the Sea (A historical perspective). U.N DIV-ì. FOR OCEAN AFF. & THE LAW OF THE SEA, 1998.

Times, New York. «New Nuclear Sub is Said to Have Special Eavesdropping Ability.» 20 febraio 2005.

V. Francola, A. Mensah. «L'Industria dei cavi sottomarini: qualche elemento introduttivo.» *Astrid Rassegna(Laboratorio sull'ecosistema digitale Astrid)*, 2021.

(C. Gerlach 2012)